

华为云泰国 PDPA 遵从性说明

文档版本 2.1
发布日期 2022-06-12



版权所有 © 华为云计算技术有限公司 2022。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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
1.1 适用范围	1
1.2 发布目的	1
1.3 基本定义	1
2 云服务的隐私保护责任界定	3
3 泰国个人数据保护法 PDPA 概述	5
3.1 法规背景介绍	5
3.2 角色划分及基本义务	5
3.3 华为云在 PDPA 下的角色	6
4 华为云如何满足泰国 PDPA	7
4.1 华为云隐私承诺	7
4.2 华为云隐私保护基本原则	7
4.3 法规基本义务及华为云相关做法	8
5 华为云如何协助客户满足泰国 PDPA	12
5.1 客户的隐私保护责任和义务	12
5.2 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	13
6 华为云隐私保护相关认证资质	17
7 结语	19
8 版本历史	20

1 概述

1.1 适用范围

本文档提供的信息适用于华为云在泰国开放的产品和服务。

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；
- 泰国隐私相关的法规；
- 基于责任模型，华为云自身关于泰国隐私法规的遵循性；
- 华为云在隐私管理上已实现的控制和成效；
- 基于责任模型，泰国隐私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泰国隐私相关的法律法规的遵从。

1.3 基本定义

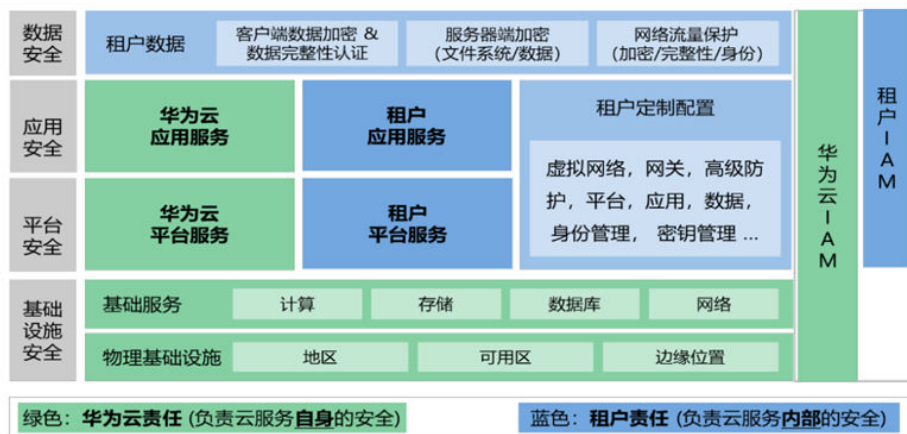
- **个人数据**
指能够直接的或间接的识别自然人的数据，但不包含死者数据。
- **数据主体**
指一个身份已被识别或者身份可被识别的自然人。
- **数据控制者**
指有权利和责任决定个人数据的收集、使用及披露的自然人或法人。
- **数据处理者**
指根据数据控制者发出的指令，对个人数据的收集、使用及披露进行操作的自然人或法人，且该自然人或法人不是数据控制者。
- **华为云**
华为云是华为的云服务品牌，致力于提供稳定可靠、安全可信、可持续创新的云服务。

- **客户**
指与华为云达成商业关系的注册用户。
- **第三方**
指数据主体、数据控制者、数据处理者以及在数据控制者或数据处理者直接授权处理个人数据者以外的自然人、法人、公共机构、行政机关或其他非法人组织。
- **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数据，华为云是控制者。
- **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。
- **处理**
是指针对个人数据或个人数据集合的任何一个或一系列操作，诸如收集、记录、组织、建构、存储、自适应或修改、检索、咨询、使用、披露、传播或其他利用，排列、组合、限制、删除或销毁，无论操作是否采用自动化的手段。

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，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。
- **数据主体权利响应**：租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 泰国个人数据保护法 PDPA 概述

3.1 法规背景介绍

2022年6月1日，泰国《个人数据保护法》（Personal Data Protection Act B.E.2562，简称PDPA）正式生效。该法对收集、保护、使用、披露、传输和其他方式处理个人数据做出了规定。

3.2 角色划分及基本义务

PDPA规定了数据控制者及数据处理者两种角色，并基于这两类角色分别规定了其义务。

- **数据控制者的基本义务包括：**
 - **获取数据主体同意：** 仅在数据主体同意的情况下收集个人数据，并通知数据主体收集数据（除非适用例外情况）的目的；仅在获得数据主体同意并告知其目的地国家或国际组织个人数据保护标准不足的情况下才能将个人数据传输到不具有足够数据保护标准的泰国境外国家或国际组织，除非存在PDPA规定的其他允许跨境传输例外情况。
 - **安全的数据处理：** 安排适当的安全措施，防止丢失、未经授权的非法访问、使用、更改和披露，包括在必要时或技术更改时对该措施进行审查。
 - **响应数据主体权利：** PDPA赋予了数据主体获取个人数据副本、撤回同意、删除、限制使用、更正的权利，当数据主体提出行使权利时，数据控制者应依照法律要求进行响应。
 - **处理活动记录：** 保留个人数据处理活动记录。
 - **防止未经授权向第三方披露或使用数据：** 除PDPA允许的未经数据主体同意的情形外，仅出于数据主体同意的目的使用和披露个人数据；与数据处理者签订个人数据处理协议，确保数据处理者遵守PDPA规定的义务。
 - **数据删除：** 个人数据到期、变得不必要时应或数据主体的要求安排删除或销毁个人数据。
 - **数据泄露通知：** 在发生个人数据违规行为后，根据PDPA的要求，通知个人数据保护委员会办公室和数据主体。
 - **指定一名DPO：** 任命一名个人数据保护专员。

- **指定一名当地代表：**如果数据控制者位于泰国境外，则需以书面形式授权任命一名泰国当地代表，全权承担任何根据数据控制者的目的而收集、使用或披露个人数据的责任。
- **数据处理者的基本义务包括：**
 - **遵循指令：**仅根据数据控制者的指示继续收集、使用或披露个人数据相关的活动。
 - **证明合规性：**遵守与数据控制者签订的个人数据处理协议。
 - **安全的数据处理：**安排适当的安全措施，防止丢失、未经授权的非法访问、使用、更改和披露。
 - **数据泄露通知：**根据PDPA要求向数据控制者告知发生的个人数据泄露事件。
 - **指定一名DPO：**任命一名个人数据保护专员。
 - **处理活动记录：**按照个人数据保护委员会规定的规则和方法，准备和保存个人数据处理活动的记录。

3.3 华为云在 PDPA 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信息。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提供的个人数据时，华为云作为数据控制者。

- **华为云作为客户个人数据的数据控制者**

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，确保数据的收集、处理、存储过程符合法律规定，响应数据主体权利申请，基于PDPA要求的有限度披露以及努力避免数据泄露事件的发生。

- **华为云作为客户内容数据的数据处理者**

当客户为数据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，华为云的角色为数据处理者。华为云代表客户根据个人数据处理协议或数据控制者指令处理个人数据，并维护数据处理的记录。

4 华为云如何满足泰国 PDPA

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完全融入到每个云服务中，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，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或组织措施确保个人数据的安全，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 法规基本义务及华为云相关做法

基于华为云业务的特性，根据泰国PDPA的要求，数据处理者与数据控制者有不同的义务，华为云积极响应并履行自身的义务。

在管理帐户信息时，华为云作为数据控制者：

法规基本义务	华为云作为数据控制者的责任	华为云的做法
获取数据主体同意	<p>确定并控制收集个人数据的时间、方式、目的、来源。确保向相关数据主体披露其收集数据的目的，并且仅出于允许目的使用数据。</p> <p>当从第三方获取数据时，需要确保来源合法可靠，并获得数据主体的同意。</p>	<p>在客户注册帐号时，提供隐私声明并获得客户的同意。</p> <p>仅基于客户同意的目的使用或披露数据。</p> <p>当产品或服务收集的个人信息范围或使用目的发生变化时，将对隐私声明进行变更，并重新获取客户的同意。</p> <p>如果购买服务或者售后服务涉及隐私声明中以外的个人信息收集或者个人信息使用目的，将在该产品的产品协议中提供额外的隐私声明，并获得数据主体的同意。</p>
安全的数据处理	<p>安排适当的安全措施，防止丢失、未经授权的非法访问、使用、更改和披露，在必要时或技术更改时对该措施进行审查。</p> <p>安全措施一般从组织、管理和技术方面开展：</p> <ul style="list-style-type: none"> • 确定企业内部信息安全的负责人或团队； • 根据自身情况，建立安全要求； • 引入安全技术保障安全要求的执行。 	<p>华为云采取严格的管理和技术控制，确保个人信息在访问、传输、存储、处理等各生命周期阶段的安全。</p> <ul style="list-style-type: none"> • 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； • 在数据处理方面，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。 <p>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 27018、BS 10012、SOC2Type1隐私原则的审计报告等（详细的认证介绍见第6章），其中ISO27018是专注于云中个人信息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信息保护管理系统。</p>

法规基本义务	华为云作为数据控制者的责任	华为云的做法
响应数据主体权利	与数据主体进行联系并与其直接沟通收集和处理其个人数据的问题，响应数据主体的权利申请并保留个人数据的处理记录。数据主体权利响应的时间及回复需要满足PDPA的要求。	华为云设立了个人信息保护专职部门。当数据主体提出行使权利时，可以通过访问 隐私问题 页面与其取得联系，华为云会尽快回复。
处理活动记录	通过日志收集和存储工具记录了数据主体的信息、收集个人数据的目的、数据控制者的信息、个人数据的保存期限、数据主体权利申请及响应的信息、执行适当安全措施的操作日志等。	<p>华为云对于隐私管理活动留存完整的活动记录：</p> <ul style="list-style-type: none"> • 在服务上线前，会执行隐私影响评估，在评估记录中会列出个人数据类型、收集个人数据的目的、个人数据保存期限。 • 在服务日常运维时，按照法规要求，保留数据主体权利申请及响应的信息和执行安全措施的操作日志。
防止未经授权向第三方披露或使用数据	<p>保证在向第三方使用和披露个人数据之前，其使用目的得到数据主体的同意。</p> <p>如果第三方是数据处理者，需签署个人数据处理协议，明确各方责任和义务、沟通方式等。确保PDPA职责的履行。</p> <p>向第三方传输数据时，使用安全的数据传输方式，避免数据在传输过程中泄露。</p>	<p>华为云在《隐私政策声明》中说明了个人数据使用的情形并获得了数据主体的同意。</p> <p>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第三方。在该情形下，华为云与需要共享数据的第三方签署了协议，并在协议中规定了个人数据处理要求，数据处理要求涉及不应将个人数据用于其他目的、使用安全管理和技术保证数据安全、数据泄露通知华为云、数据主体权利响应协助等。</p> <p>当传输个人数据给第三方时，华为云将使用加密传输，保证数据传输过程的安全。</p>
数据删除	<p>确保个人数据到期时删除个人数据。</p> <p>当个人数据变得不必要时删除个人数据。</p> <p>当数据主体提出删除请求时，应按照法规要求删除相应数据。</p>	<p>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。</p> <p>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。</p>
数据泄露通知	在得知数据泄露事件后72小时内向个人数据保护委员会办公室报告个人数据违规行为。	华为云设置7x24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。
指定一名DPO	任命一名内部个人数据保护专员。	华为集团设立了全球数据保护官岗位，其岗位责任范围覆盖华为云国际站业务。

在处理内容数据时，华为云作为数据处理者：

法规基本义务	华为云作为数据处理者的责任	华为云的做法
遵循指令	<p>确保仅根据数据控制者的指示继续收集、使用或披露个人数据相关的活动。</p>	<p>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。</p> <p>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。</p>
安全的数据处理	<p>安排适当的安全措施，防止丢失、未经授权的非法访问、使用、更改和披露，在必要时或技术更改时对该措施进行审查。</p> <p>安全措施一般从组织、管理和技术方面开展：</p> <ul style="list-style-type: none"> ● 确定企业内部信息安全的负责人或团队； ● 根据自身情况，建立安全要求； ● 引入安全技术保障安全要求的执行。 	<p>华为云主要负责底层云的安全以及产品本身的隐私安全：</p> <ul style="list-style-type: none"> ● 在底层云安全中，华为云基础设施提供了最佳可用性和完整的客户隔离，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底层的安全性。底层云强大的信息安全能力奠定了云上隐私安全的坚实基础。 ● 客户可以通过华为云安全标准类的认证验证华为云环境中的安全控制，包括 ISO 27001、CSASTAR金牌认证、PCI-DSS等认证。 ● 在产品本身的隐私安全中，华为云服务从需求设计到运营运维整个生命周期全过程执行隐私保护管控。需求分析过程中，对隐私需求和相关法律法规分析，将安全和隐私需求优先纳入服务规划中；设计阶段，梳理涉及的所有个人数据类型并记录，通过PIA方法识别潜在风险并将风险控制措施融入到服务设计中；开发阶段，通过编码静态扫描及隐私安全编码检视，确保开发过程及编码符合公司相关的开发规范；在测试阶段，所有隐私特性需通过严格测试并经过专家团队审视，确保隐私需求和设计在云服务中实现。 ● 云服务隐私保护合规不仅限于研发阶段，在服务持续运维运营阶段，华为云通过各项技术和管理措施保证个人数据不被非授权访问和处理，保障数据主体权利，确保云服务持续的隐私安全。 ● 客户也可以通过华为云隐私类认证和报告验证华为云环境中的隐私安全控制，包括 ISO 27701、ISO 29151、ISO 27018等。

法规基本义务	华为云作为数据处理者的责任	华为云的做法
数据泄露通知	在得知数据泄露事件后72小时内向个人数据保护委员会办公室报告个人数据违规行为。	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。
处理活动记录	通过日志收集和存储工具记录了数据主体的信息、收集个人数据的目的、数据控制者的信息、个人数据的保存期限、数据主体权利申请及响应的信息、执行适当安全措施的操作日志等。	按照PDPA规定的规则和方法，准备和保存个人数据处理活动的记录，包括： <ul style="list-style-type: none"> ● 在涉及个人数据的服务上线前，华为云会执行隐私影响评估，在评估记录中会列出个人数据类型、收集个人数据的目的、个人数据保存期限。 ● 在涉及个人数据的服务上线后，客户要求华为云提供数据主体权利响应、故障处理等协助时，华为云将保留自身操作的记录。

5 华为云如何协助客户满足泰国 PDPA

5.1 客户的隐私保护责任和义务

当客户是数据控制者且华为云协助处理客户内容数据中个人数据时，客户有可能满足 PDPA 管辖条件。如若满足，客户应承担 PDPA 要求的隐私保护责任，同时华为云将尽自己最大的努力帮助客户实现隐私安全。

法规基本义务	客户作为数据控制者的责任	华为云如何帮助客户
获取数据主体同意	<p>确定并控制收集个人数据的时间、方式、目的、来源，并决定是否将个人数据通过华为云存储或处理。客户需要确保向相关数据主体披露其收集数据的目的，并且仅出于允许目的使用数据。</p> <p>当从第三方获取数据时，需要确保来源合法可靠，并获得数据主体的同意。</p>	<p>部分华为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主体的要求。例如客户可通过华为云提供的接口嵌入客户的隐私政策并记录相关操作记录。</p>
安全的数据处理	<p>安排适当的安全措施，防止丢失、未经授权的非法访问、使用、更改和披露，在必要时或技术更改时对该措施进行审查。</p> <p>安全措施一般从组织、管理和技术方面开展：</p> <ul style="list-style-type: none"> • 确定企业内部信息安全的负责人或团队； • 根据自身情况，建立安全要求； • 引入安全技术保障安全要求的执行，安全技术可以使用华为云提供的安全配置，也可以使用自己的安全工具或者第三方解决方案。 	<p>华为云产品中提供访问控制，网络隔离等安全配置。</p> <p>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，如统一身份认证服务、云监控服务、数据加密服务、Web 应用防火墙、虚拟专用网络、虚拟私有云、数据库安全服务、DDoS 高防 AAD、漏洞扫描服务等。</p>

法规基本义务	客户作为数据控制者的责任	华为云如何帮助客户
响应数据主体权利	与数据主体进行联系并与其直接沟通收集和处理其个人数据的问题，响应数据主体的权利申请并保留个人数据的处理记录。数据主体权利响应的时间及回复需要满足PDPA的要求。	华为云有专门的团队保证和客户的沟通联系，客户可以通过工单服务寻求华为云的帮助。
处理活动记录	通过日志收集和存储工具记录了数据主体的信息、收集个人数据的目的、数据控制者的信息、个人数据的保存期限、数据主体权利申请及响应的信息、执行适当安全措施的操作日志等。	华为云提供了 云日志服务 、 云审计服务 、 云硬盘备份 以及 云服务器备份 ，帮助客户方便快捷的收集、分析日志，及时发现隐私处理风险。
防止未经授权向第三方披露或使用数据	保证在向第三方使用和披露个人数据之前，其使用目的得到数据主体的同意。 如果第三方是数据处理者，需签署个人数据处理协议，明确各方责任和义务、沟通方式等。确保PDPA职责的履行。 向第三方传输数据时，使用安全的数据传输方式，避免数据在传输过程中泄露。	-
数据删除	确保个人数据到期时删除个人数据。 当个人数据变得不必要时删除个人数据。 当数据主体提出删除请求时，应按照法规要求删除相应数据。	华为云在服务和产品中提供可删除个人数据的功能。
数据泄露通知	在得知数据泄露事件后72小时内向个人数据保护委员会办公室报告个人数据违规行为。	华为云有专门的团队保证和客户的沟通和联系，客户可以通过工单服务寻求华为云的帮助。
指定一名DPO	任命一名内部个人资料保护专员。	-
指定一名代表	如果数据控制者位于泰国境外，则需以书面形式授权任命一名泰国当地代表，全权承担任何根据数据控制者的目的而收集、使用或披露个人数据的责任。	-

5.2 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

华为云深刻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从PDPA。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	对应的隐私保护义务
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您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。	安全的数据处理
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、资源变更、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，保障数据主体的知情权、实现快速查找	处理活动记录
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。	安全的数据处理
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，保障数据主体的知情权。	处理活动记录

• **安全产品**

产品名称	产品介绍	对应的隐私保护原则
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。	安全的数据处理

产品名称	产品介绍	对应的隐私保护原则
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。	安全的数据处理
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。	安全的数据处理
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。	安全的数据处理
DDoS高防 (AAD)	AAD是一款保护互联网服务器免受大流量DDoS攻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。	安全的数据处理

• 网络产品

产品名称	产品介绍	对应的隐私保护原则
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。	安全的数据处理

产品名称	产品介绍	对应的隐私保护原则
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，各租户之间100%隔离，增强云上数据的安全性。	安全的数据处理

• 数据存储产品

产品名称	产品介绍	对应的隐私保护原则
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。	处理活动记录
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。	处理活动记录

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、贯穿个人数据处理全生命周期的管理措施。
- **ISO 27018**
云平台个人数据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数据保护措施的要求，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 认证表明华为云在个人数据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 and 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
- 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

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。华为云具备业界领先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，帮助客户轻松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泰国PDPA的遵从性。

8 版本历史

日期	版本	描述
2022年6月	2.1	法规生效
2022年4月	2.0	合规要求更新
2020年8月	1.0	首次发布