

华为云隐私保护白皮书

文档版本 2.0
发布日期 2021-01-22



版权所有 © 华为技术有限公司 2021。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

引言

随着云计算技术和云服务的不断演进和成熟，公有云、混合云等各种模式的云服务逐渐成为越来越多的企业的最佳选择。云服务提供商为企业带来更便捷、更丰富、也更经济实惠的云服务，如何保护云上数据、尤其是个人数据的安全，不仅是云服务提供商的首要任务，也逐渐成为企业业务上云的主要考量因素。

2016年11月，中国颁布了《中华人民共和国网络安全法》，对个人信息保护提出一系列要求。关于个人信息保护的国家级标准《信息安全技术 个人信息安全规范》也于2018年正式实施。中国的个人信息保护法正在制定中，目前已发布草案。2016年，欧盟发布《通用数据保护条例》（General Data Protection Regulation，以下简称GDPR）并于2018年5月正式生效，对个人隐私权利提出了明确的法律要求。GDPR的一经发布即在全球范围内产生了深远影响，公众对隐私保护的关注达到空前高度。近年，阿根廷、新西兰、巴西、印度、土耳其、泰国等国家也相继发布了本国隐私保护法律。全球范围内对个人隐私保护的监管日益严格，不仅对云服务提供商的隐私保护提出了更高要求，也客观上使得企业（尤其是开展跨国业务的企业）的隐私保护合规工作将更具挑战。

华为云是华为的云服务品牌，将华为30多年在ICT领域的技术积累和产品解决方案开放给客户，致力于提供稳定可靠、安全可信、可持续创新的云服务。华为云在隐私保护方面付出诸多努力并取得了显著的成效，我们希望借此白皮书与您分享将华为云的隐私保护理念和相关工作，介绍我们如何保护客户的个人数据，以及华为云服务如何帮助客户构建云上的隐私保护。

目 录

引言.....	ii
1 概述.....	1
2 隐私保护合规和认证.....	2
2.1 合规性.....	2
2.2 标准与认证.....	3
3 共同构筑隐私安全.....	4
3.1 华为云的责任.....	4
3.2 客户的责任.....	5
4 华为云如何管理和保护数据隐私.....	6
4.1 个人数据处理基本原则.....	6
4.2 华为云隐私保护管理体系.....	6
4.3 技术和工具.....	9
5 客户如何保护云上业务的隐私安全.....	11
5.1 DevSecOps——云服务生命周期管控.....	11
5.2 云服务的隐私安全特性.....	12
5.3 相关云服务.....	12
6 结语.....	14
7 版本历史.....	15

1 概述

网络安全和隐私保护^①一直是华为生存之本，从创立至今，华为人便一直坚定地朝着这个方向不懈努力。基于华为公司在网络安全和隐私保护方面多年的实践与经验，华为云充分理解隐私的重要性，现已将隐私保护融入到每个云服务中。在以网络安全和隐私保护为公司最高纲领的指导下，华为云以“**尊重和保护隐私，让人们放心地使用便捷可信的云服务**”为愿景。围绕这一愿景，华为云郑重对待网络安全和隐私保护事项并积极承担相应责任，设置了专业的隐私保护团队，制定并完善隐私保护管理流程，积极研发安全和数据保护技术，不断建设和提升华为云隐私保护的能力，**为客户提供稳定可靠、安全可信、可持续演进的云服务。**

得益于华为云全方位、系统性的隐私保护管理体系的支撑，使得我们可以更好地实现这一目标。华为云以全球隐私保护的法律法规为基石，参考业界广泛认可的优秀实践，建设华为云的隐私保护体系。华为云投入大量的专业人员和资源，支撑管理措施和信息技术的研究和落地，保障隐私保护体系的有效运转，确保华为云的隐私保护合规并获得持续发展。

当然，实现隐私保护需要强大的安全能力为其提供支撑，隐私保护和安全息息相关。华为云在云安全方面具备行业领先的实践和积累，详细内容请查看《[华为云安全白皮书](#)》和《[华为云数据安全白皮书](#)》。

华为云秉承数据中立态度，严守服务边界，保障数据为客户所有、为客户所用、为客户创造价值；华为云承诺将确保相关业务遵从业务所在国家/地区适用的隐私保护法律法规。

^① 隐私：最广泛的定义是个人let alone的权利。物理上隐私是指个人住宅或个人财产、搜身、监控或提取生物特征信息，而信息性的隐私是指个人控制、编辑、管理和删除关于自己信息的能力和决定如何与他人沟通这些信息的能力。本白皮书中主要谈及的是信息性的隐私。

2 隐私保护合规和认证



2.1 合规性

法律遵从是企业开展业务的合规底线，华为云遵守业务所在地所有适用的法律法规要求。华为云投入专业的法务团队，紧密关注全球范围内华为云服务适用的法律法规更新情况，对相关法律法规保持持续跟踪并进行快速分析，确保华为云业务合规。对部分云服务网络安全、隐私保护相关的法律、法规及行业监管要求，我们结合华为云服务特性编写了合规遵从白皮书，以说明华为云对特定法律法规要求的遵从性，帮助客户理解适用法律法规要求并为全球客户在不同国家业务的隐私合规性提供参考。

截止目前，华为云已发布十余份各国隐私保护法律或行业标准遵从白皮书，并将持续发布更多的白皮书，您可以随时在华为云官方网站信任中心获取到以下白皮书^②：

[巴西LGPD合规性说明](#)

[马来西亚PDPA合规性说明](#)

[新加坡PDPA合规性说明](#)

[华为云泰国PDPA合规性说明](#)

[华为云南非POPIA合规性说明](#)

[中国香港特别行政区PDPO合规性说明](#)

[华为云HIPAA合规性说明](#)

[华为云PCI DSS 实践指南](#)

[新加坡金融行业监管要求合规性说明](#)

[中国香港金融行业监管要求合规性说明](#)

[泰国金融行业监管遵从性指导](#)

2.2 标准与认证

华为在践行业界网络安全和隐私保护领域优秀实践的同时，积极加入如云安全联盟、IAPP等国际权威组织，参与各类云安全和隐私保护标准的起草和修订，将华为的实践和经验回馈社会和全行业。华为云网络安全和隐私保护的能力和成效在全球范围得到广泛认可。目前，华为云共取得海内外十余家机构的第三方认证。

下面列举了华为云已获得的部分与隐私保护强相关的认证^③：

ISO/IEC 27018:2014

ISO/IEC 29151:2017

ISO/IEC 27701:2019

BS 10012:2017

ISO/IEC 27799

PCI DSS认证

PCI-3DS认证

可信云服务用户数据保护能力认证（中国）

SOC 2 Type I/II Report（隐私性）

华为云积极关注业界权威隐私认证机制的出台，并持续提高要求，完善隐私保护体系，增加和更新安全和隐私方面的认证。同时，华为云和隐私保护相关协会紧密合作，对隐私保护前沿资讯及技术进行探讨，帮助华为云打造一个可持续发展的、安全可信的云平台环境。

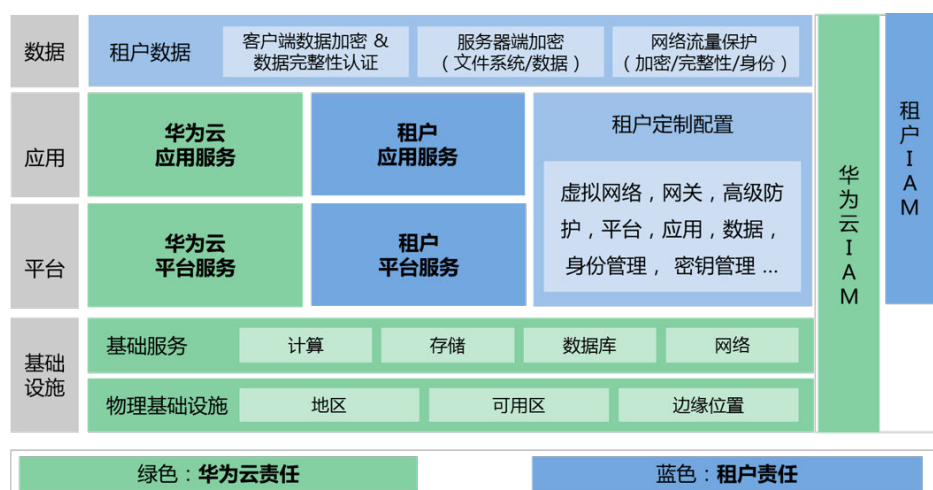
② 华为云可能随时新增或更新隐私合规性白皮书，所有信息以华为云官网发布内容为准。相关文件您可以在华为云官网信任中心获取最新版本：<https://www.huaweicloud.com/securecenter/resource.html>。

③ 客户进行相关认证时，如需从华为云获得必要的协助，可访问华为云信任中心获取华为云相关认证证书的副本：<https://www.huaweicloud.com/securecenter/compliance.html>。

3 共同构筑隐私安全

华为作为云服务提供商（CSP）向客户提供了基础设施即服务（IaaS），平台即服务（PaaS）和软件即服务（SaaS）各类云服务，在复杂的云服务环境中如何实现隐私安全，需要客户与华为云共同努力。隐私保护对企业提出了明确的要求，本章我们将基于以下责任模型介绍客户在使用云服务时需要承担的隐私保护责任和义务，以及华为云如何帮助你更好的实现隐私安全。

图 3-1 华为云安全责任共担模型



如上图所示，华为云主要负责云服务自身的安全以及合规，并为客户提供在数据处理、存储、转移等过程中的所需的隐私特性。针对客户内容数据^④，客户拥有全部的权利和义务，包括隐私保护的义务，制定安全和隐私保护策略和措施确保个人数据^⑤安全，保障数据主体权利^⑥以及各项活动合规。

该模型帮助客户理解华为云和客户各自承担的隐私保护责任和义务，有利于客户识别其个人数据，制定合适的个人数据保护策略，从而最终更好地实现隐私保护。

基于责任模型，华为云与客户主要承担如下的隐私保护责任：

3.1 华为云的责任

华为云作为云服务提供方，负责构建由基础设施层、平台层、应用层组成的云平台，并负责云平台基础设施如物理环境、软硬件、计算、网络、数据库、存储等以及平台

层、应用层的安全。华为云各项活动和云服务遵从隐私保护相关法律法规，为客户提供稳定、安全和有利于隐私保护的云环境。

华为云为客户提供多种隐私保护技术，包括访问控制和身份认证、数据加密、日志和审计和其他相关的隐私保护技术，以及基于此基础上的华为云各项服务，帮助客户根据业务需求进行隐私保护。华为云拥有完善的隐私保护体系和多方位的隐私保护管控机制，能实现华为云隐私保护的责任。

3.2 客户的责任

客户对其内容数据拥有全面控制权，应正确、全面地识别云端的个人数据，选择恰当的服务并制定安全和隐私保护策略以保护个人数据安全。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。客户可使用华为云为其提供的多种隐私保护服务，例如使用数据识别技术对数据进行识别和分类、使用访问控制服务对个人数据设置最小权限并按需分配权限、使用加密手段对个人数据的存储和传输进行保护等。

客户应保障其数据主体的权利，响应数据主体请求，当发生个人数据泄露事件时，通知数据主体并采取相应措施。客户可使用华为云为其提供的多种隐私保护服务，例如使用日志功能，保留对个人数据的操作记录，以帮助保障其用户对个人数据的知情权。客户应确保其对个人数据处理符合隐私保护相关法律法规的要求。对此，华为云提供多种隐私保护服务及合规解决方案，帮助客户实现全面的隐私保护合规。

④ 客户内容数据：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。

⑤ 个人数据/个人信息：指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，其主要包括：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。

⑥ 数据主体权利：数据主体依法对其个人数据享有的各项权利，包括但不限于知情权、访问权、数据可携带权、被遗忘权等。

4 华为云如何管理和保护数据隐私

4.1 个人数据处理基本原则

在云服务中，我们讨论隐私保护的绝大部分场景是关于信息化的个人数据的处理，我们如何保护保障数据主体相关的权利以及如何保护个人数据的安全性。为此，我们确定了个人数据处理的基本原则，并通过适当的管理和技术措施确保在处理个人数据时遵从以下基本原则。

合法 正当 透明

处理个人数据的方式必须是合法、正当、对数据主体透明的。

目的限制

收集个人数据的目的必须是具体的、明确的、合法的，且不能超出此种目的对个人数据进行进一步处理。

数据最小化

仅收集和处理与数据处理目的相关的、必要的、适当的个人数据。存储或使用个人数据时尽可能进行匿名化或化名处理，降低对数据主体的风险。

准确性

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

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，在业务活动完成后，即对个人数据删除或匿名化处理。

完整性与保密性

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

遵从上述原则并保留相关数据处理记录，且必要时可对外展示证明对上述原则的遵从性。

4.2 华为云隐私保护管理体系

为保护客户个人信息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^⑦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。本章后续内容将从几个重要的方面介绍华为云如何管理隐私保护工作。

组织和人员管理

华为云成立了专门隐私保护团队，明确业务的隐私保护责任人，并持续提升相关人员的隐私保护意识和能力，以支撑华为云业务中实现默认的隐私保护。

- **隐私保护组织**

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。在各产品、服务的业务团队中，华为云设置专门的隐私保护角色，负责云服务的隐私保护合规与能力建设。在各个业务所在国家和地区，华为云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。

- **人员管理**

华为云从多方面确保全体员工资质、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核确保员工符合要求。当员工不再负责当前工作时，相关权限将被删除。

- **意识和能力提升**

华为云通过多种形式的培训定期为全员提供隐私保护意识培训，以加深员工对隐私保护的理解和对华为隐私保护政策规定的了解。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。对于特殊岗位如涉及接入客户网络或数据处理的人员，根据岗位性质和风险，将开展定制的隐私保护技能培训和考试，只有通过考核后方能上岗。

流程框架

华为云在各业务领域广泛应用PbD理念，将隐私保护基本原则全面融入到相关业务流程中，以期在业务开展之前即考虑隐私保护，实现默认的隐私保护。华为云已建立全面的隐私保护流程体系，通过发布隐私保护政策和目标统一思想 and 认识，发布管理规定和流程要求明确业务规范，并配套相应的操作指导、工具和模板等以帮助工作人员合规且高效的开展业务活动。确保在华为云业务活动开展中落实隐私保护基本原则，切实保护个人数据的安全，保障数据主体相关的权利。

隐私风险管理

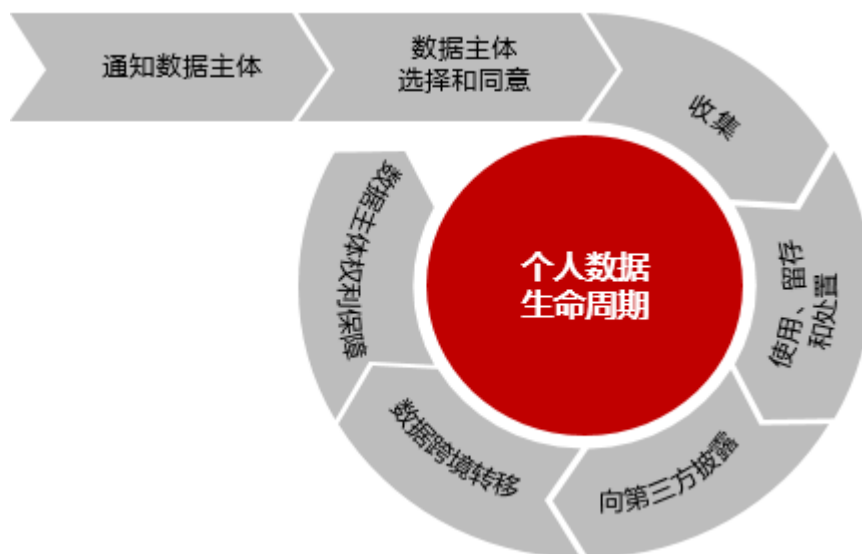
为有效地识别和控制隐私风险，华为云在云服务各项业务中广泛地开展隐私风险分析和管理工作。华为云要求在所有业务处理个人数据前必须开展隐私风险分析（PIA），主要包括识别业务涉及的个人数据项、业务场景及处理过程、合规分析、对数据主体可能产生的影响、风险分析并制定风险控制措施和计划等，只有将隐私风险降低至可接受的水平后才能开展业务。

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。

个人数据处理全生命周期管理

为更好地保障数据主体权利与保护个人数据安全，华为云将个人数据处理基本原则贯彻到个人数据处理各个阶段，明确个人数据处理全生命周期的管控要求，并将这些要求融入到所有业务活动中。

图 4-1 个人数据生命周期



- **通知、选择和同意、收集**

华为云仅在获得客户的同意后，收集提供服务所必须的客户的个人数据，同时提供隐私通知告知客户所收集的个人数据类型、目的、处理方式、时间等内容。如在官网提供隐私政策声明以及客户同意及撤销同意的机制。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。华为云在其官网上提供丰富的配置选项，客户可根据偏好设置接收消息的种类和方式。针对涉及个人数据处理相关特性的云服务，华为云在其产品资料中，告知客户关于个人数据的种类、处理和存储的方式等相关信息，客户可根据产品资料的信息采取相应的隐私保护措施。

- **使用、留存和处置**

华为云对留存在华为云平台上的个人数据，采取严格的管控措施，为了确保个人数据的安全，对个人数据的接入、认证、授权、存储、审计进行统一管理。华为云制定了明确的留存时间，在超出数据处理所需要的时间，个人数据将被自动删除。华为云对运维人员权限实行基于角色的访问控制权限管理，根据岗位需求授予相应的权限并进行定期监控确保访问权限与岗位需求相匹配。华为云定期对日志进行回溯审计，对人员操作行为进行审阅以检查对个人数据操作的合理性和必要性。

- **第三方披露**

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》。

- **数据跨境转移**

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客户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。

- **数据主体权利保障**

华为云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^⑧，当接收到客户问题请求后在规定时间内完成响应和请求处理，反馈处理结果给客户。华为云隐私保护团队，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。

4.3 技术和工具

华为云对客户个人数据安全非常重视，在管控机制和技术上采取了先进，严格的管控，确保客户个人数据安全。



技术研究和应用

信息技术的发展日新月异，华为在技术研究方面始终保持着高投入，并持续将新技术运用于网络安全和隐私保护领域。如通过访问控制和身份认证相关技术的应用，实现权限“最小必要原则”，对系统权限实现数据级、操作级的精确管控；华为云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记录对各关键系统的访问和操作和对密钥的使用等，定时进行监控和审计，及时发现和纠正隐私保护方面可能存在的的行为；同时分析潜在的隐私保护和个人数据安全隐患以便及时迅速的做出反馈，解决问题。同时，华为云持续将这些技术应用于保护客户的个人数据以及华为云提供的各项云服务中，以更好地保护客户的个人数据。

隐私保护技术（PET）

华为云技术团队同时致力于研发各类隐私保护技术，积累隐私保护工程技术能力，实施隐私保护以满足客户不同需求。华为云现已拥有的一系列PET，包括等价类匿名、差分隐私、防跟踪技术、区块链私人支付以及隐私保存计算等。

- **数据屏蔽**

华为云的数据屏蔽技术通过包括掩码、加噪、枚举、截断、哈希、标志化等手段，防止从数据中关联用户身份及敏感信息，对个人数据的单个字符的屏蔽来保护数据隐私，降低数据泄露的风险。

- **差分隐私**

差分隐私是一种加噪算法，在保留数据一定的可用性，又能保证攻击者无法推断出某个用户的信息。差分隐私在不知道数据库本身内容的情况下，注入“噪声”。从而数据集进行模糊化处理，但不影响统计结果。可在数据库查询时，减少个人数据被识别的几率。

- **可搜索加密**

可搜索加密技术可实现对加密状态下的个人数据进行搜索，如客户的邮箱、电话号码、身份证号等加密存储的个人数据，可以在不明文显示的情况下进行搜索处理，降低个人数据泄露风险。

工具

华为云使用多种隐私保护平台工具，帮助华为云更快速、系统、高效地处理与隐私保护相关的各项工作。

- **数据发现和管理**

数据发现工具可以帮助我们识别系统、数据库或者文件里的个人数据，以了解业务是否包含个人数据以及个人数据的类型和流转情况等相关的信息，同时也可以帮助我们采取恰当的隐私保护措施（具体可参看[DBSS](#)、[DSC服务](#)）。数据管理服务可以帮助华为云完成数据资产注册和管理，对个人数据清单的记录、全生命周期管理提供工具化的能力。

- **隐私风险分析**

将隐私保护风险分析全过程工具化，可帮助各个业务团队通过标准化的流程和工具识别隐私保护风险并制定和实施相应的风险处置措施。

⑦ PbD: Privacy by design, 隐私融入设计方法（PbD）最早作为针对产品研发周期隐私保护的方法。经过近几年的发展，逐渐演变成隐私保护的管理理念。PbD提倡全面、提前、主动将隐私保护融入业务和各项活动中，帮助组织在隐私保护中取得主动地位。

⑧ 隐私问题请求：客户可以通过华为云官网提交[隐私问题请求](#)或privacy@huaweicloud.com 邮箱 与华为云隐私保护团队取得联系，以沟通或报告隐私保护相关的问题。

5 客户如何保护云上业务的隐私安全

华为云深刻理解保护个人数据对客户的重要性，并努力地采取管控措施和提供相应的服务帮助客户保护其个人数据安全。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，并向客户提供丰富的安全服务以满足租户不同安全级别的要求，详情可参考华为云已发布的《华为云数据安全白皮书》。

5.1 DevSecOps——云服务生命周期管控

从IaaS、PaaS到SaaS众多的云服务是客户在云上构建业务的基础，华为云深知云平台和云服务自身的隐私安全是客户实现云上业务隐私安全的基石。如在云服务研发中，为保证云服务实现默认的隐私保护特性，华为云将安全融入DevOps，全面实施DevSecOps流程，在云服务生命周期各个阶段都将安全和隐私融入其中。我们采取严格隐私保护要求和控制措施，以确保云服务具备保护个人数据的安全能力，同时充分满足客户隐私保护的需求，帮助客户保护其用户的隐私。下图列举了我们在云服务生命周期中部分主要的隐私保护控制点。

图 5-1 云服务生命周期及隐私管控



华为云在每个云服务生命周期采取的隐私保护管控措施，以实现：

- 全生命周期贯彻PbD的理念，使每个云服务本身满足隐私合规要求，同时具有隐私保护特性。
- 严格测试和审查，确保隐私合规需求得到实现、隐私保护特性的有效。
- 对隐私保护的要求不止步于产品上线，在运营运维的阶段，通过人员及流程的管控，为客户提供合规的云服务，帮助客户实现其隐私保护。

5.2 云服务的隐私安全特性

华为云通过严格的研发流程管控使所有华为云服务具备默认的安全和隐私特性，如：

- **隐私通知**

对于涉及个人数据处理的云服务，我们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，以帮助客户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，客户可根据业务合规需求自行配置隐私通知。

- **加密**

如果客户的业务数据中涉及敏感个人数据，云服务将默认加密存储该等数据，在非信任网络之间的传输的数据都是被加密的。同时，部分云服务还为客户提供了自助控制的选项，客户可以根据自身需求选择是否加密存储数据，或者使用何种加密方法对数据进行加密。在使用华为云服务时你还可以通过专门的加密服务管理你的数据加密。

- **权限控制**

访问控制和权限管理是实现隐私保护的基本要求，所有的云服务都被要求集成统一身份认证服务，并且在云服务使用中验证用户身份和权限。

- **日志审计**

可追溯是华为云隐私保护的基本原则，日志记录也是华为云服务的基本特性。客户可以通过云服务自身的日记记录特性来满足业务对日志记录的需求，还可以同时配套华为云CTS服务使用，以支撑日志审计、相关的合规要求。

华为云服务的安全和隐私保护特性远不止于此，以上仅列举了一些典型的特性，其他如数据最小化、同意和撤销同意、存留期限等一系列可以体现华为云服务PbD理念的服务特性不再赘述，可通过[华为云官网](#)资料了解详细内容。

5.3 相关云服务

除了上节所述隐私特性，华为云还为客户提供了综合的隐私保护解决方案和丰富的云服务，以帮助客户构建和提升云上业务的安全和隐私保护水平。客户可根据自身业务特点选用相关的隐私服务，管理和保护个人数据。

统一身份认证服务（IAM）

统一身份认证服务（Identity and Access Management）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）账号，并且可以控制这些用户对您名下资源的操作权限。

数据加密服务（DEW）

数据加密服务（Data Encryption Workshop）是一个综合的云上数据加密服务。它可以提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块（HSM）保护，并与许多华为云服务集成。用户也可以借此服务开发自己的加密应用。

数据安全中心（DSC）

数据安全中心服务（Data Security Center）是新一代的云原生数据安全平台，提供数据分级分类，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能力，通

过数据安全总览整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势。

数据库安全服务（DBSS）

数据库安全服务（Database Security Service）是一个智能的数据库安全防护服务，基于反向代理及机器学习机制，提供敏感数据发现、数据脱敏、数据库审计和防注入攻击等功能，保障云上数据库的安全。

云日志服务（LTS）

云日志服务（Log Tank Service）提供一站式日志采集、秒级搜索、海量存储、结构化处理、转储和可视化图表等功能，满足应用运维、网络日志可视化分析、等保合规和运营分析等应用场景。

审计服务（CTS）

云审计服务（Cloud Trace Service）为您提供云账户下资源的操作记录，通过操作记录您可以实现安全分析、资源变更、合规审计、问题定位等场景。您可以通过配置OBS对象存储服务，将操作记录实时同步保存至OBS，以便保存更长时间的操作记录。



更多华为云服务，可访问以下华为云产品页面获取：

<https://www.huaweicloud.com/product>。

6 结语

华为云在海内外的业务日渐壮大，为客户提供智能、安全、可信的云服务面临更多、更高要求。华为云始终秉持“**以客户为中心**”的核心价值观，充分理解和尊重客户的隐私权利，切实保护客户个人数据的安全；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合规要求。

秉承公司网络安全和隐私保护的最高纲领，华为云将继续践行隐私保护愿景和目标，持续为客户提供安全可靠的云服务，帮助客户保护个人数据。华为云始终保持开放态度，不断研究学习、与多方合作，取长补短，持续提升和丰富华为云安全和隐私保护服务和能力，在帮助客户创造价值的同时，与客户共同维护云环境下个人的隐私保护权利。

华为云希望借此白皮书的发布，分享在隐私保护的实践和经验，也希望能与客户继续并肩同行，共同创造安全、可信、透明的云环境。



更多关于华为云隐私保护内容和服务，请访问华为云官网：

<https://www.huaweicloud.com/>。

7 版本历史

日期	版本	描述
2019年7月	1.0	首次发布
2021年1月	2.0	例行刷新