中资出海欧洲监管要求遵从性指南

文档版本 1.0

发布日期 2026-07-30



华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2026。 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



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/intl/zh-cn/**

目 录

1 概述 2
1.1 背景与发布目的 2
1.2 名词定义 2
2 华为云安全与隐私合规 5
3 华为云责任共担模型 8
4 华为云全球基础设施 10
5 中资出海欧洲安全合规重点 11
5.1 适用的监管要求简介 11
5.2 出海合规路径 13
5.3 欧洲安全合规重点要求 13
6 华为云如何遵从及协助客户满足欧洲安全合规要求 25
6.1 出海前，建立安全治理体系 25
6.2 出海中，管控产品交付与供应链安全 32
6.3 出海后，保障稳定运营与外部沟通 41
7 华为云为客户提供的安全与隐私保护相关的云服务 44
8 结语 48
9 版本历史 49

1 概述

1.1 背景与发布目的

随着国内企业持续布局欧洲市场，各类跨境云端业务不断落地开展，企业在日常经营、产品服务交付过程中，均会大量收集、存储与处理欧盟境内用户的个人数据。为规范相关数据与数字化业务运营，欧盟陆续出台 GDPR、AI Act、CRA、NIS2、CSA 2.0 草案等多项监管法规，从个人数据保护、产品安全管控、供应链风险管理、人工智能合规治理等多个维度，对开展相关业务的企业明确了全面、严格的监管约束与法定责任。

华为云作为云服务供应商，致力于协助国内企业客户满足这些监管要求，持续为出海企业提供符合欧盟监管标准的云服务及业务运行环境。本文将围绕欧洲出海云场景，说明双方的安全责任共担框架、欧盟法规核心义务，并详细介绍华为云如何依托平台、工具与服务，帮助国内企业在出海全阶段达成合规、压缩合规成本，稳定开展跨境业务。

1.2 名词定义

- **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。

- **云服务**

  是指云服务提供商根据用户请求，通过互联网以云计算模式提供的 IT 服务和计算资源，根据计算模式可将云服务分成基础设施即服务（Infrastructure-as-a-Service，IaaS）、平台即服务（Platform-as-a-Service，PaaS）、软件即服务（Software-as-a-Service，SaaS）三类。

- **云服务提供者**

  指向公共行政部门提供云服务的公私主体，其亦可通过分销商、经销商或增值服务提供者提供服务，但前述中介在不决定服务交付方式和手段的情况下，不被视为云服务提供者。

- **个人数据**

  指任何与已识别或可识别的自然人（“数据主体”）相关的信息。

 版权所有 © 华为云计算技术有限公司

- **处理**

  指对个人数据执行的任何操作，无论是否采用自动化方式，如收集、记录、存储、使用、披露、删除等。

- **数据控制者**

  指单独或与他人共同决定个人数据处理目的和方式的自然人或法人。

- **数据处理者**

  指代表控制者处理个人数据的自然人或法人。

- **数据主体**

  指其个人数据被处理的自然人。

- **同意**

  指数据主体自由作出的、具体的、知情的和明确的意愿表示，通过声明或明确的肯定行动表明同意处理其个人数据。

- **假名化**

  指一种处理个人数据的方式，使其在不结合额外信息的情况下无法再关联到特定数据主体，且该额外信息需分开存储并受技术和组织措施保护。

- **人工智能系统**

  基于机器的系统，旨在以不同级别的自主性运行，部署后可表现出适应性，并为了明确或隐含的目标，从接收到的输入中推断如何生成输出，如预测、内容、建议或决策，从而影响物理或虚拟环境。

- **高风险人工智能系统**

  （1）作为产品安全组件，或本身即为产品，且需根据欧盟协调法规接受第三方合格评估的 AI 系统；

  （2）法案附件三所列特定领域（如生物识别、关键基础设施、教育、就业等）中对自然人健康、安全或基本权利构成重大风险的系统。

- **通用人工智能模型**

  一种在大量数据上训练的 AI 模型，具有显著通用性，能够胜任多种不同任务，无论其以何种方式投放市场。

- **提供者**

  指开发 AI 系统或以自己名义/商标将 AI 系统投放市场的自然人或法人。

- **部署者**

  指在其授权下使用 AI 系统的自然人或法人，但不包括个人非职业活动中的使用。

- **带有数字元素的产品**

  指任何软件或硬件产品，及其远程数据处理解决方案，其预期用途或合理可预见的使用涉及直接或间接的逻辑或物理数据连接。

 版权所有 © 华为云计算技术有限公司

- **软件物料清单**

  一份记录构成软件产品的组件及依赖关系的正式结构化文件，是产品安全文档的一部分。

- **漏洞**

指信息技术产品中可被威胁利用的弱点、缺陷或程序错误。

- **制造商**

指开发或制造带有数字元素的产品，并以自身名义或商标将其投放市场的自然人或法人。

- **CE 标志**

一种物理或数字标志，制造商将 CE 标志贴附于产品，即表明其承担该产品符合欧盟协调法规所规定所有适用要求的责任。

- **关键实体**

指属于 NIS2 指令附件 I-高度关键部门所列行业，如能源、交通、医疗、数字基础设施等，并达到特定规模门槛的公共或私营实体。

- **网络和信息系统**

指一组相互连接或关联的、通过程序自动处理数字数据的设备，或用于其运行、使用、保护和维护的数字数据存储、处理、检索或传输设施。

- **安全事件**

指任何危害网络和信息系统可用性、真实性、完整性或保密性的事件。

- **重大事件**

指能够或可能对实体服务提供造成严重运营中断或重大经济损失，或对其他自然人或法人造成重大物质或非物质损害的事件。

- **托管安全服务提供商**

指为其他实体提供或协助提供与网络安全风险管理相关服务的实体，如安全事件响应、渗透测试、安全审计等。

- **进口商**

指设立于欧盟境内的自然人或法人，将带有欧盟境外主体名称、商标的带数字元素产品投放欧盟市场。

- **分销商**

指供应链内除制造商、进口商以外的自然人或法人，在不改变产品属性的前提下，于欧盟市场提供带数字元素产品流通。

 版权所有 © 华为云计算技术有限公司

2 华为云安全与隐私合规

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
ISO 27001	ISO 27001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。
ISO 27017	ISO 27017是针对云计算信息安全的国际认证。ISO 27017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。
ISO 27018	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。
ISO 42001	ISO/IEC 42001是全球首个人工智能管理体系标准，该标准提供了一个可认证的人工智能管理体系（AIMS）框架，为组织建立、实施、维护和持续改进人工智能管理体系提供要求和指南，旨在帮助组织和社会负责任地开发、提供和使用AI系统，并从人工智能中受益。
ENS	ENS（西班牙语：Esquema Nacional de Seguridad，ENS）是西班牙国家安全认证计划，其通用框架分为基本原则、控制要求和安全措施三个部分。ENS适用于所有西班牙公共部门以及与西班牙政府合作的供应商。认证的目的是确保组织管理的数据、信息和服务在机密性、完整性、可追溯

 版权所有 © 华为云计算技术有限公司

认证	描述
	性、真实性和可用性五个维度中得到充分保护。
C5	C5全称Cloud Computing Compliance Criteria Catalogue（云计算合规标准目录），是由德国联邦信息安全办公室（BSI）针对云服务商制定的安全标准，旨在基于标准化的检查和报告来说明云服务提供商的信息安全性。C5目前已经广泛地被欧洲乃至全世界的企业使用，是云服务领域受到充分认可的高级别安全标准。C5:2020基于《欧洲网络安全法》对云服务产品的信息安全标准进行了延伸（e.g. 标准化云服务提供商处理政府机构查询的行为），提升了服务提供商行为的规范和严谨性。
EU Cloud CoC	《欧盟云行为准则（EU Cloud CoC）》是欧洲数据保护委员会（EDPB）签署的跨国运营合规行为准则，旨在为云服务商提供明确的指导，帮助其遵守《通用数据保护条例（GDPR）第28条-数据处理者》规定的义务。 获得《欧盟云行为准则》认证可作为云服务商面向欧盟监管机构和云用户的合规证明。 该合规性工具适用于提供不同云服务模式的各种规模的企业。
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。 TL 9000是一个建立在ISO 9001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ISO 9001的所有要求，ISO 9001将来的任何改动也会导致TL 9000的改动。 华为云取得了ISO 9001 / 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。
ISO 20000	ISO 20000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。
ISO 22301	ISO 22301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	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。
ISO 27701	ISO 27701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ISO 27701表明了其在个人

 版权所有 © 华为云计算技术有限公司

认证	描述
	数据保护具有健全的体制。
BS 10012	BS 10012是BSI发布的个人信息数据管理体系标准，BS 10012 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	ISO 29151是国际个人身份信息保护实践指南。ISO 29151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。
ISO 27799	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。 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。

 版权所有 © 华为云计算技术有限公司

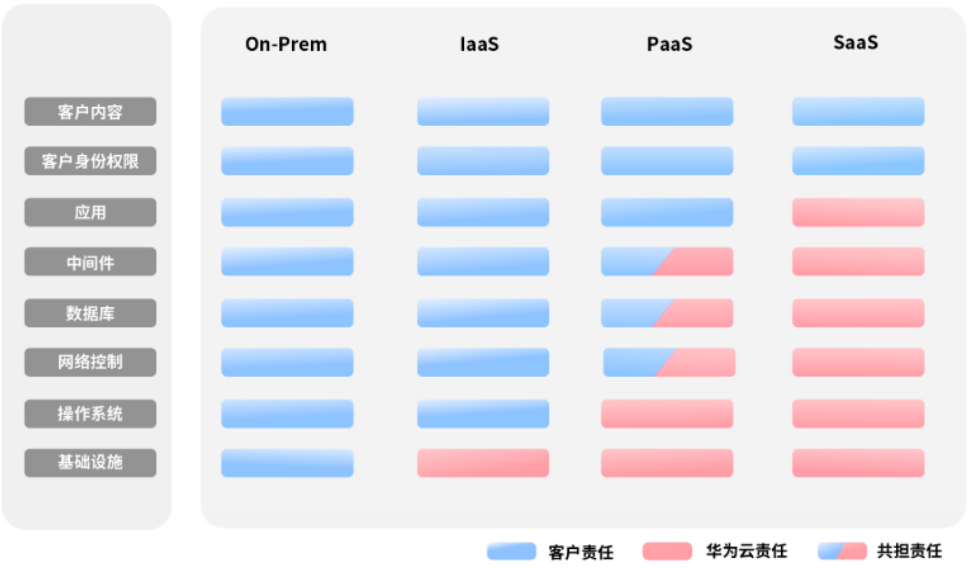
3 华为云责任共担模型

客户在云上业务的安全性与合规性是华为云与客户的共同责任。与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。也正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与客户共同努力。

云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产(例如设备、硬件、软件、介质、虚拟机、操作系统、数据等)由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如下图所示，客户可以基于自身的业务需求选择不同的云服务类别(例如 IaaS、PaaS、SaaS服务)。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

在监管要求可能适用于客户内容的情况下，“责任共担”模型帮助华为云和客户双方理解各自角色以及责任。

图 3-1 华为云责任共担模型



华为云的责任：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心(计算、存储、网络 等)、

 版权所有 © 华为云计算技术有限公司

虚拟化平台及云服务组成。在 PaaS、SaaS 场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。

客户的责任：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转 移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证(如强口令、多因子认证)并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

在 On-prem 场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。

在 IaaS 场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件(如中间件、数据库和操作系统)的漏洞修复、配置安全、安全防护方案等。

在 PaaS 场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。

在 SaaS 场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

 版权所有 © 华为云计算技术有限公司

4 华为云全球基础设施

华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域(Region)和多可用区(AZ)的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。更多关于华为云基础设施的信息，参见华为云官网“**全球基础设施**”。



 版权所有 © 华为云计算技术有限公司

5 中资出海欧洲安全合规重点

5.1 适用的监管要求简介

欧洲议会和欧盟理事会（THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION）：欧洲议会是欧洲公民的直接代表，也是欧洲联盟的中央立法机构；欧盟理事会在欧盟决策中发挥着重要作用，欧盟理事会与欧洲议会合作，通过普通立法程序协商和通过立法法案。

欧盟委员会（European Commission）是欧盟常设执行机构与立法提案主体，致力于起草法案草案、监督法规执行与统筹政策落地。其总体目标是维护欧盟整体利益，保障欧盟法律体系有效运转与统一实施。

- **《通用数据保护条例》（General Data Protection Regulation，GDPR）**:2018年5月25日，欧盟议会和欧盟理事会发布该条例，该条例确立合法、公正、透明、目的限制、数据最小化、存储限制等个人数据保护基本原则，并对所有处理个人数据的经营主体制定统一且严苛的合规规范。
- **《人工智能法案》（Artificial Intelligence Act，AI Act）**：2024年3月14日欧洲议会通过、同年8月2日生效，是全球首部综合性AI监管法案。法案按风险将AI系统分为四类，高风险AI相关义务2026年8月起实施，具备域外管辖效力。2026年5月修订案延长高风险AI合规过渡期，并新增相关管控条款，旨在管控AI风险、保障公民权益、规范可信AI创新。
- **《网络弹性法案》（Cyber Resilience Act，CRA）**:2024年10月10日，欧盟理事会正式通过该法案，2025年生效、2027年全面实施，该法案为欧盟首部面向数字产品全生命周期安全的强制法规，对进入欧盟市场的软硬件产品设置全周期网络安全硬性要求，规定企业需落实SBOM清单、漏洞上报、CE认证等义务。
- **《网络与信息安全指令第二版》（Directive on Security of Network and Information Systems 2，NIS2）**:2022年12月14日，欧洲议会和欧盟理事会发布该指令，2024年1月17日正式实施，该指令作为欧盟关键基础设施网络安全核心法规，替代旧版NIS指令，拓宽适用行业范围，覆盖能源、交通、医疗、数字基础设施等领域，对相关主体提出网络安全风险管控、安全事件上报、供应链防护等强制要求，法规管辖所有在欧盟提供服务的关键经营主体，不受企业总部所在地限制。
- **《网络安全法案2.0》（Cybersecurity Act 2026年提案）**:2026年5月，欧盟委员会提出该立法草案，该法案作为欧盟网络安全体系补充法规，聚焦ICT产业链安全

 版权所有 © 华为云计算技术有限公司

治理，覆盖软硬件厂商、云服务商、关键基础设施运营方等主体，建立供应链全流程安全管控机制，强制企业落实供应链风险评估、供应商安全审计等工作，强化跨境安全协同，守护欧盟数字生态安全稳定。

- **《数据法案》（Data Act）**:2024 年 1 月生效，是欧盟继 GDPR 后又一核心数据立法。法案重点规范数据访问与共享，强制网联产品及相关服务进行 B2C 和 B2B 数据共享，要求数据持有者以公平、合理、非歧视（FRAND）原则提供数据，便利用户切换数据处理服务，并防范非法国际政府数据访问。法案适用于在欧盟市场投放网联产品的制造商、服务提供商、数据持有者及数据处理服务商等（不论其注册地），大部分义务条款自 2025 年 9 月起实施。
- **《云与人工智能发展法案》（Cloud and AI Development Act, CADA 2026 年提案）**:2026 年 6 月，欧盟委员会推出“技术主权一揽子计划”，CADA 是该计划的核心立法提案之一，聚焦云与 AI 领域的研究创新、数据中心能力建设及主权保障，旨在提升欧盟在云和 AI 领域的自主可控能力，为数字主权与安全治理提供重要支撑。
- **《数字运营韧性法案》（Digital Operational Resilience Act, DORA）**:2022 年 12 月 14 日发布，2025 年 1 月 17 日生效，是欧盟针对金融行业的数字运营韧性专门立法。法案要求金融机构有效管理 ICT 风险，并将关键 ICT 第三方服务提供商纳入统一监管框架，确保金融体系在严重运营中断下维持稳定运行。
- **《网络安全及网络安全管理体系》（UNECE R155，Cyber security and cyber security management system）**:是全球首部针对汽车信息安全的强制性法规，由联合国欧洲经济委员会（UNECE）的世界车辆法规协调论坛（WP.29）于 2021 年 1 月生效，旨在为全球道路车辆的网络安全型式批准提供统一框架。
- **《关于批准车辆的软件升级和软件升级管理体系统一规定的法规》（UNECE R156，Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system）**:2021 年 1 月生效，是全球首部专门针对汽车软件升级的强制性国际法规，核心是要求车辆制造商必须建立并维护一个软件升级管理体系。它与 UNECE R155 共同构成了车辆网络安全与软件更新的两大支柱。

作为领先的云服务提供商，华为云深刻洞察欧盟市场法规环境的复杂性与持续演进态势，已建立起覆盖全球的安全合规体系。面对《通用数据保护条例》（GDPR）、《人工智能法案》（AI Act）、《数据法案》（Data Act）、《网络弹性法案》（CRA）、《网络与信息安全指令第二版》（NIS2）及《数字运营韧性法案》（DORA）等密集出台的法规要求，华为云持续加大合规投入，深化能力建设。

面向特定行业领域，华为云已推出多份专业白皮书与遵从性指南——金融行业涵盖**《数字运营韧性法案（DORA）监管要求遵从性指南（欧盟）》**及**《金融行业监管要求遵从性指南》**；汽车行业发布了**《欧洲汽车行业安全与隐私合规遵从指南》**。

当前，华为云将正式发布《中资出海欧洲监管要求遵从性指南》，重点围绕 GDPR、AI Act、CRA、NIS2 及 Cybersecurity Act(草案)五部核心法规，全面阐释华为云在数据保护、人工智能治理、网络弹性、网络安全风险管理及 ICT 供应链安全等维度的合规能力与产品应对策略，为中资企业提供系统性的合规指引。上述这五大法案的合规要求，已成为中资企业顺利开拓欧盟市场的必备前提。华为云将持续输出合规知识与实践指引，助力中资企业在欧洲市场合规运营、稳健发展。

 版权所有 © 华为云计算技术有限公司

5.2 出海合规路径

企业出海欧盟市场，为应对《通用数据保护条例》、《人工智能法案》、《网络弹性法案》、《网络与信息安全指令第二版》及《网络安全法案 2.0》草案等多部数字法规，企业合规工作主要分布在数据合规隐私保护、AI 系统合规、网络与产品安全三大领域，可按出海前中后三个阶段系统推进：



图：出海业务全生命周期安全合规框架

企业出海合规工作覆盖出海前、出海中、出海后全流程：

- 出海前需完成法规适用性分析、安全合规风险分析、安全治理组织与政策流程优化、供应商尽职调查及协议签署，重点落实安全治理管理、风险管控、数据安全隐私保护及人员合规意识建设；
- 出海中开展数据中心、网络、应用、数据全生命周期与 AI 安全架构设计，实施上线前安全测试调优、供应商常态化安全管理并办理投产所需安全许可，核心关注开发部署、交付运维、供应链管理、AI 安全以及安全许可与合规销售；
- 出海后持续开展安全监测、安全事件响应处置、合规度量与第三方认证审计，重点做好长期安全隐私有效性验证以及面向监管、第三方机构的外部沟通工作。

5.3 欧洲安全合规重点要求

欧盟安全合规要求贯穿企业出海业务的全生命周期，是进入欧盟市场的强制性准入门槛。下表基于出海前、中、后三个阶段，系统梳理企业在数据合规与隐私保护、AI 系统合规、网络与产品安全三大领域需落实的合规义务。

序号	合规重点	适用的具体要求	出海阶段
1	安全治理与管理	**在数据合规隐私保护方面，欧盟要求明确数据控制者的合规问责义务，划定数据保护官（DPO）强制设立场景、岗位职责与独立履职保障要求。**	出海前

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
	（GDPR 第 24 条、第 37-39 条 AI Act 第 4 条、第 17 条 NIS2 第 20 条 CRA 第 13 条、第 28 条）	• 明确数据控制者问责义务。控制者需建立配套管理机制，保障全部数据处理活动符合 GDPR 规范，并留存材料以证明合规状态。 • 划定数据保护官（DPO）法定设立情形。公共机构开展数据处理、实施大规模监控行为、大规模处理健康、生物识别等特殊类别数据时，控制者与处理者应当设置 DPO。 • 规范 DPO 核心工作职能。为管控主体提供 GDPR 合规指引、监督内部合规落地、提供数据保护影响评估专业意见，同时作为对接监管机构、数据主体的官方沟通渠道。 设定 DPO 履职保障要求。控制者需保障 DPO 独立开展工作，不得施加不合理工作指令，同时配置充足人力、技术、资金资源支撑职责履行。	
		在AI系统合规方面，AI法案对高风险AI系统提供者提出全流程质量管理体系建设要求，明确体系建设主体、必备合规模块及体系融合规则。 • 体系覆盖产品设计、开发、部署全流程，由企业管理层主导建设、实施与持续改进。 • 体系需完整纳入 AI 法案合规要求，包含合规策略、风险管理、数据治理、技术文档、记录留存、投用监测及事件报告。 该体系可整合至ISO 9001等现有企业管理体系，但须充分满足 AI 法案专项合规要求。	出海前
		在网络与产品安全方面，欧盟要求 **1、明确基本实体与重要实体管理层的网络安全管理职责、法律责任、惩戒机制及能力建设要求。** • 落实管理层主体责任。企业董事会、执行管理层需审批网络安全风险管理措施、监督落地执行，并对法案第 21 条违规行为承担个人法律责任。 • 明确管理层惩戒规则。针对严重违反 NIS2 义务的行为，成员国可对相关管理层人员采取临时撤销任职资格等惩戒措施。 • 规范管理层履职能力与管理要求。管理层需定期参与网络安全专项培训，具备安全风险评估与业务影响研判能力；需确保网络安全风险管控适配业务运营需求，并将网络安全纳入企业整体战略。 **2、明确制造商管理层的产品合规最终责任，落实管理层在符合性声明、产品管控、体系运维方面的核心职责。** • 管理层承担产品合规最终责任，秉持审慎原则保障产品全面符合 CRA 要求，确保技术文档完整、安全更新及时交付。 • 管理层对欧盟符合性声明的真实性负责并完成签字确认。 • 管理层需建立并常态化运维符合 CRA 规范的质量管理体系与漏洞处置流程。 **3、明确企业管理层供应链风险监督职责，划定治理落地与资源保障相关要求。**	出海前

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
		• 管理层应将供应链映射、高风险供应商排查纳入企业治理体系，全面监督供应链风险。 • 管理层需为高风险供应商组件的淘汰替代计划配置充足财务、技术与人力资源，并建立内部审计机制，持续监督供应链合规状态。	
2	风险管理（GDPR 第 35 条 NIS2 第 21 条 CRA 第 13 条 + 附件一）	**在数据合规隐私保护方面，欧盟要求若数据处理活动（尤其依托新技术开展）会对自然人权利与自由形成高风险，数据控制者必须在开展处理工作前完成数据保护影响评估（DPIA）**。 完整评估报告需包含四项核心内容： • 待实施数据处理活动的完整梳理说明； • 处理行为合规性、必要性综合研判； • 数据主体各项权益面临的风险等级评估；clash • 配套落地的风险防控与缓释方案。 出现以下场景时，企业必须强制开展 DPIA： • 针对自然人开展大规模、持续性自动化画像评估； • 大批量处理健康、生物识别等特殊类别敏感个人数据； • 在大范围公共区域部署持续性视频监控采集数据。	出海前
		在网络安全合规方面，欧盟要求： **1、核心实体与重要实体应采用适配、均衡的技术、运维及组织管控手段管控网络安全风险。**相关防护措施需覆盖十大维度： • 风险分析与信息系统安全管理制度 • 安全事件处置（监测、应急响应与业务恢复） • 业务连续性保障（备份管控、灾备恢复、危机处置） • 供应链安全管理 • 网络与信息系统全生命周期安全（采购、开发、运维、漏洞处置与披露） • 风险管理措施有效性评审制度与流程 • 基础网络安全规范与全员安全培训 • 密码算法落地与加密管理规范 • 人员安全管理、权限访问策略、资产管控 • 多因素认证 / 持续身份核验、安全音文字通信、应急通信体系 **2、搭载数字功能产品的生产厂商，需在产品设计研发阶段结合已识别风险同步开展安全内置设计，产品上市前完成覆盖用途、使用场景、运行环境、核心资产及全生命周期的网络安全风险评估，相关评估资料统一归档留存。**在产品合规管控上，分为两大核心维度： • 上市前置合规要求，产品需消除可利用已知漏洞，全面落实安全默认配置、权限管控、数据加密、完整性保护、数据最小化、可用性保障、操作审计追溯等安全机制； • 上市后全生命周期管控要求，常态化开展 SBOM 清单管理、安全漏洞修复与安全检测，严格执行漏洞披露规范，建立健全常态化安全事件处置体系。	出海前

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
3	数据安全与隐私保护（GDPR 第 5 条、第 6 条、第 9 条、第 13-22 条，第 32 条 AI Act 第 10 条、第 50 条、第 53 条第 15 条 NIS2 第 21 条 CRA 第 13 条 附件一）	**在数据合规隐私保护方面，欧盟要求:** **1、数据控制者与处理者落实适配的技术与组织安全措施，明确措施范畴与安全水平的判定依据，保障个人数据全流程安全。** • 安全措施需覆盖个人数据假名化与加密，保障处理系统与服务的保密性、完整性、可用性与韧性，具备物理或技术故障后的数据恢复能力，并建立定期测试、评估措施有效性的流程。 • 安全水平的确定需综合考量现有技术成熟度、实施成本，以及数据处理的性质、范围、场景与目的等因素。 **2、规定个人数据处理的基础准则、合法依据、特殊数据管控、数据主体权利及隐私告知规范。** • 数据处理遵循七项基础原则：合法公正透明、目的限制、数据最小化、准确性、存储期限限制、完整保密、可举证问责。 • 开展数据处理需满足六类合法基础之一：数据主体同意、履约所需、法定义务、保护生命权益、公共职能、合法利益（主体权利优先除外）。 • 特殊类别数据原则禁止处理，仅书面同意、医疗诊疗、公共利益等法定例外场景可开展处理。 • 赋予数据主体六项法定权利：访问、更正、删除、限制处理、数据携带、反对处理，同时享有拒绝无人工干预自动化决策的权利。 • 控制者需出具清晰易懂的隐私声明，完整表明主体信息、处理目的、合规依据、接收方、留存周期、主体权利及投诉渠道。 **3、明确个人数据跨境传输的合规路径、使用限制、前置义务与禁止条款。** • 跨境数据传输需适用三类合法机制其一：欧盟充分性认定；SCC、BCR、认证、行业准则等适当保障措施；法定特殊例外场景。 • 特殊例外严格受限：无充分认定与保障措施时方可适用，且仅限个案，禁止常态化使用。 • 跨境传输前置义务：事前评估第三国数据保护法制环境并留存评估记录；采用保障措施传输时，向数据主体提供保障文件副本。 • 禁止条款：不得通过多层流转数据规避 GDPR 保护要求。	出海前
		在AI系统合规方面，欧盟要求高风险 AI 系统在全生命周期内保持合规的准确性、鲁棒性与网络安全水平，明确各维度落地标准。 • 准确性层面，提供者须在技术文档中载明系统在预期用途下的准确性指标。 • 鲁棒性与网络安全层面，系统需具备抵御运行错误、误用及对抗性攻击的能力，同时配置与风险等级匹配的防护机制，防范模型反演、对抗样本、数据投毒等 AI 专项攻击。	出海前

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
		在网络与产品安全方面，欧盟要求 **1、基本实体与重要实体落实十大类体系化安全管控措施，筑牢网络安全防护屏障。** • 管控范畴覆盖多因素/持续认证、加密技术、业务连续性管理、备份恢复、访问控制、人员安全、网络安全培训等核心维度。 • 具体执行需满足明确标准：采用强加密算法保护静态及传输中的数据，严格落实最小权限访问控制；定期开展数据备份并测试恢复流程，制定业务连续性与灾难恢复专项计划；面向员工开展网络安全意识培训，内容涵盖钓鱼邮件识别与基础安全规范。 **2、欧盟对带有数字元素的产品明确全维度安全合规要求，由制造商负责落实，覆盖产品技术防护与数据全生命周期管理两大层面。** • 构建产品全流程网络安全防护体系。设计阶段融入网络安全原则，出厂默认禁用不安全协议与非必要服务；依托认证机制落实访问控制，通过冗余设计、DDoS 防护保障服务可用性，采取关闭冗余端口与服务、部署 ASLR/DEP 及栈保护等手段压缩攻击面、缓解漏洞风险；同步记录关键安全事件日志，保障日志的机密性与完整性。 • 执行全生命周期数据安全管控规范。采用行业认可的加密算法保护静态与传输中数据，通过数字签名、哈希校验机制防范未经授权的数据篡改；严格遵循数据最小化原则，仅收集实现预期目的的必要数据并向用户明确说明收集范围与用途；支持安全数据删除与跨系统安全传输功能，确保已删除数据不可恢复，数据传输全程落实加密与完整性保护措施。 **3、欧盟对带有数字元素产品的制造商明确产品支持周期与安全更新管理规则，保障产品全生命周期持续满足安全合规要求。** • 明确支持期设定与告知标准。产品支持期自上市起不得少于 5 年，若产品预期使用周期更短，制造商需出具对应技术依据；支持期需于产品上市前确定，在用户说明中标注起止时间，并明示期满后不再提供安全更新的风险。 • 规范安全更新交付与留存要求。支持期内须免费持续推送安全更新以修复漏洞，且安全更新需与功能更新明确区分；安全更新发布后，需按“至少 10 年或支持期剩余时长”取较长期限留存归档，供用户下载。 • 划定违规处置边界。若支持期内未按要求推送必要安全更新，用户或主管机构可要求相关产品下架。	出海前
4	人员与意识（AI Act 第 4 条）	**在AI系统合规方面，欧盟要求AI系统提供者与部署者明确人员AI素养建设义务，区分通用建设要求、高风险系统专项责任与供给方支撑义务，确保人员能力匹配岗位需求与系统风险等级。** • 系统提供者与部署者双方需针对直接使用、开发、监督及管理 AI 系统的全链条相关人员，配套适配的素养提升措施；措施需结合使	出海前

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
		用者技术背景、应用场景与系统风险等级制定，并随技术迭代持续更新。 • 高风险 AI 系统的部署者须承担专项责任，确保操作人员可准确理解系统输出、及时识别误用或故障、有效履行人类监督职责。 AI 系统提供者需向部署者提供必要的培训材料与相关信息，支撑企业内部 AI 素养建设落地。	
5	开发与部署（CRA 第 13 条、附件二、第 19-20 条）	**在网络与产品安全方面，欧盟要求** **1、对数字产品制造商设置全流程文档编制、用户安全告知及长期留存义务，强化产品全生命周期安全可追溯性。** • 制造商需编制覆盖设计、开发、生产、投用全阶段的技术文档，包含网络安全风险评估、软件物料清单（SBOM）、安全测试审查结果、漏洞处理流程记录；同步编写通俗化用户使用说明，列明产品预期用途、安全功能、厂商信息、服务支持周期、安全更新与配置指引、漏洞报送渠道等内容。 • 技术文档与欧盟符合性声明副本，需自最后一件产品投放市场起留存 10 年，以备市场监管机构调阅核查。 **2、法规对数字产品制造商设置全流程文档编制、用户安全告知及长期留存义务，强化产品全生命周期安全可追溯性。** • 制造商需编制覆盖设计、开发、生产、投用全阶段的技术文档，包含网络安全风险评估、软件物料清单（SBOM）、安全测试审查结果、漏洞处理流程记录；同步编写通俗化用户使用说明，列明产品预期用途、安全功能、厂商信息、服务支持周期、安全更新与配置指引、漏洞报送渠道等内容。 • 技术文档与欧盟符合性声明副本，需自最后一件产品投放市场起留存 10 年，以备市场监管机构调阅核查。	出海中
6	交付与运维（GDPR 第 30 条 AI Act 第 11-12 条、第 71 条 NIS2 第 21 条、第 23 条	**在数据合规隐私保护方面，欧盟要求对个人数据处理活动记录作出明确规范，区分控制者与处理者设置差异化留存要求，并配套相应豁免规则。** • 控制者及其代表（如有）需以书面或电子形式留存处理活动记录，内容涵盖主体身份与联系方式、处理目的、数据及主体类别、接收方范围、跨境传输保障措施、数据留存期限及技术与组织安全措施概述。 • 处理者需就受托开展的全部处理活动类别留存记录，内容要求与控制者基本一致，无需载明处理目的。 雇员规模不足 250 人的企业原则上可豁免记录义务，但若处理活动可能侵害数据主体权利、属于非偶发处理，或涉及特殊类别数据、刑事定罪相关数据的，仍需履行记录义务。	出海中

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
	CSA 2.0 第 110 条）	**在AI系统合规方面，欧盟要求对高风险 AI 系统构建全生命周期合规监管体系，覆盖入市合规自证、运行追溯管控与监管备案登记全流程。** • 提供者须在系统投放市场前完成技术文档编制并持续更新，文档涵盖系统概况、预期用途、风险管理体系、研发数据与方法、验证测试结果、准确性指标及网络安全措施等，用以证明系统符合 AI 法案全部要求。 • 系统需具备自动日志记录功能以保障可追溯性，完整留存风险事件、系统重大变更等信息，留存时长与系统预期用途相匹配。 • 提供者须完成欧盟高风险 AI 系统数据库注册，提交主体信息、系统说明、符合性声明及第三方认证机构信息（如有）等材料。	出海中
		在网络与产品安全方面，欧盟要求 **1、对基本实体与重要实体明确网络安全文档留存要求，确保风险管理与事件处置全程可追溯、可核验。** • 主体需留存风险管理措施落地文档及网络安全事件调查报告，保存期限遵循各成员国法律规定，通常为 1 至 5 年； • 留存文档须能够佐证相关风险管理措施的合规执行，事件场景下可向主管机构提供完整调查材料以供审查。 **2、法规明确企业供应链映射记录的留存与动态管理要求，支撑监管层面的审计与风险评估工作。** • 企业须留存供应链映射记录，内容涵盖 ICT 组件来源国、供应商所有权结构、关键资产依赖关系、单一供应商依赖程度及替代供应商可用性等信息。 • 相关记录需配合欧盟及成员国的审计、风险评估工作，并在供应商或合同状态发生变更时及时更新。 **3、法规对进口商、分销商两类流通主体设定全流程合规管控义务，明确入市核验、文档留存与异常处置要求，保障上市产品符合监管标准。** • 进口商需保障第三国进口产品合规：投放市场前核查制造商符合性评估完成情况、技术文档齐备性与 CE 标志加贴情况，在产品或随附文件中标注自身主体信息；留存用户资料、使用说明及符合性声明副本 10 年，接受监管调阅；判定产品不合规时禁止其上市，并通报制造商与市场监管机构。 • 分销商需履行审慎核验责任：产品上市前确认其带有 CE 标志、全套合规文档及使用说明；发现产品不合规则禁止上市，同步通知制造商与进口商；知悉产品存在严重安全问题时，及时告知相关方并配合监管落实纠正措施。	出海中

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
7	供应链安全管理（GDPR 第 28 条 AI Act 第 10 条、第 53 条 NIS2 第 21 条第 2 款 d 项、第 22 条 CSA 2.0 第 99 条、第 110 条 CRA 附件一 第二部分 CSA 2.0 第 110－111 条）	**在数据合规隐私保护方面，法规对数据控制者委托第三方处理数据作出完整约束，明确双方权责、协议规范与持续管控要求。** • 控制者仅可委托具备专业能力、可信度达标的数据处理者开展业务，双方需签署书面数据处理协议（DPA），载明数据处理范围、周期、用途及数据、数据主体类型； • 协议约定处理者仅遵照控制者指令操作，落实配套安全防护，配合响应数据主体诉求，合约终止后返还或清除全部数据； 控制者需定期核查处理者安全合规水平，处理者未经书面许可，不得擅自分包委托次级处理者。	出海中
		在AI系统合规方面，高风险 AI 系统数据集管控及通用 AI 模型信息披露两项合规要求。 • 高风险 AI 系统服务商需规范训练、验证、测试数据集管理，核查数据来源、采集方式、标注质量与潜在偏见，并管控偏见风险，杜绝模型输出产生歧视后果； • 通用 AI 模型供应方需向下游提供模型名称、版本、能力、使用约束、训练数据概要等信息，保障下游主体履行《AI 法案》合规义务。	出海中
		在网络与产品安全方面，欧盟要求 **1、建立供应链安全管控机制，明确关键主体管控义务与监管层协同评估机制，实现供应链风险全链路覆盖。** • 基本实体与重要实体须将供应链安全纳入整体风险管理框架，核查直接供应商及服务提供方的安全能力，在采购与供应商管理环节落地风险评估结论，持续监控供应商合规状态，保障全链条安全可控。 • 欧盟合作小组联合欧盟委员会与ENISA，针对特定关键ICT服务、系统及产品开展协同安全风险评估，评估兼顾技术与非技术因素，将第三国不当影响风险纳入考量范畴。 **2、明确企业在 ICT 供应链风险管控中的两项核心义务，全面支撑欧盟层面的协同监管与风险评估工作。** • 企业须配合欧盟开展的 ICT 供应链协调性安全风险评估，按要求提供必要供应链信息，参与相关数据收集与审核工作； • 企业需建立供应链映射制度，系统性记录 ICT 组件来源国、供应商所有权结构、单一供应商或组件依赖风险等信息，保障欧盟层面风险评估与审计工作顺利推进。 **3、欧盟对企业 ICT 供应链设置全链条管控规则，明确映射管理、高风险供应商处置及风险缓释三项合规要求。** • 企业须建立供应链映射制度，系统性记录 ICT 组件来源国、供应商所有权结构、单一供应商依赖程度及替代供应商可用性等信息；	出海中

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
		• 若供应商被欧盟委员会列入高风险供应商（HRV）清单，企业须立即停止新采购、新合同签订及现有合同延期，并在清单公布后 36 个月内完成关键资产中高风险组件的拆除与替换； • 企业需制定供应商多元化策略，降低供应链中断风险。 **4、数字产品制造商建立软件组件全量管理与协同漏洞披露双重机制，落实产品全生命周期安全管控义务。** • 制造商须建立产品全组件（含第三方、开源组件）及已知漏洞的识别登记流程，编制通用机器可读格式的软件物料清单（SBOM），完整列明所有软件组件、版本、许可证及依赖关系。 • 制造商须制定协同漏洞披露政策，为安全研究人员开放公开报送渠道，及时处置并响应漏洞报告，同时跟踪、修复第三方组件中发现的安全漏洞。	
8	AI 安全（AI Act 第 9 条,第 51-56 条）	**在 AI 安全领域，** **1、欧盟要求对通用 AI 模型实行分级监管，以风险等级匹配差异化合规义务，系统性风险模型适用更为严格的管控要求。** • 明确系统性风险模型判定规则与程序。满足技术评估认定为高影响力、欧盟委员会认定具备同等能力或影响、训练计算量超 10^{25}次浮点运算法定推定情形之一的，归为系统性风险模型；模型达标后需于两周内通报欧盟委员会并提交材料，相关主体可举证抗辩以排除该认定。 • 所有通用 AI 模型均需履行基础合规义务。包括编制并动态更新技术文档，向下游主体提供模型信息与使用约束，制定欧盟版权合规使用政策，公开发布训练内容摘要。 • 系统性风险模型需承担额外专属义务。需开展覆盖网络攻击、偏见、有害内容等风险的全生命周期评估与缓释，建立严重事件上报机制，落实高水平网络安全防护，防范权重泄露、对抗性攻击等安全风险。 **2、欧盟要求高风险AI系统提供者搭建、落地、留存文档并持续运维覆盖 AI 全生命周期的风险管理体系。** 该体系需满足以下要求： • 识别并评估系统正常使用、可预见误用情形下，对人身健康、公共安全与公民基本权利造成的各类风险； • 结合系统上线后的持续监测数据，补充识别新增风险； • 配套执行风险处置手段，缓释各类已识别风险； 定期对整套风险管理制度开展全面复核与迭代更新。	出海中

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
9	安全许可与销售（AI Act 第 43 条、第 47-48 条 CRA 第 28 条、第 30 条、第 32 条 NIS2 第 24 条 CSA 2.0 第 40-52 条）	**在 AI 安全领域，欧盟对高风险 AI 系统明确入市前符合性评定规则，覆盖评估实施、声明出具与标识加贴全流程，保障系统符合 AI 法案监管要求。** • 实行差异化评估机制。高风险 AI 系统投放市场或投入使用前须完成符合性评估：采用协调标准或共同规范的系统，可开展基于内部控制的自我评估；未使用协调标准或涉及极高风险应用场景的系统，须由通知机构参与实施第三方评估。 • 规范合规声明管理。评估通过后，提供者须出具欧盟符合性声明，载明提供者信息、系统唯一识别信息、合规声明内容及授权签名，确认系统符合 AI 法案全部要求。 • 明确 CE 标志加贴要求。须在系统本体、包装或随附文件上加贴 CE 标志，标志需清晰可见、易于辨认且不可磨灭。	出海中
		在网络与产品安全方面，欧盟要求 **1、对带有数字元素的产品明确入市前符合性评定全流程要求，按产品类别与风险等级实施差异化评估机制，保障产品符合 CRA 监管标准。** • 实行分级分类符合性评估程序。一般产品可采取基于内部生产控制的自我评估；重要产品 Class I 在完全适用协调标准的前提下可自我评估，否则需通知机构参与；重要产品 Class II 及关键产品强制要求通知机构参与评估。 • 规范欧盟符合性声明管理。评估通过后，制造商须起草符合性声明，载明制造商信息、产品识别信息、合规声明内容、支持期及授权签名。 • 明确标识与可追溯要求。产品须加贴 CE 标志以证明符合 CRA 基本要求，同时需标注制造商名称与邮寄地址，保障产品可追溯。 **2、对基本实体和重要实体的合规认证实施可选认证、差异化审查机制，明确 ECCF 认证效力，兼容国际通用安全标准。** • 确立 ECCF 认证合规效力。成员国可要求相关实体采用 ECCF 认证的 ICT 产品、服务及流程，用以证明符合法案第 21 条网络安全要求；通过 ECCF 认证可产生合规推定，直接认定满足安全要求，显著简化监管审查流程。法规同时鼓励企业参考 ISO/IEC 27001 搭建风险管理体系。 • 明确双向合规路径。ECCF 认证为非法定强制要求：选择 ECCF 认证可享受合规推定、减轻核查负担；不采用 ECCF 的主体，可依据 ISO/IEC 27001 等标准自建安全体系并自查，但无法获得合规推定，需接受监管机构全面审查。 **3、实体级网络安全态势认证面向企业整体安全能力评估，具备合规减负作用，并明确认证性质与评估边界两大核心规则。**	

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
		• 认证价值与定位。该认证评估组织整体网络安全水平，区别于单一产品、流程类认证；取得认证可作为履行 NIS2、CRA 合规义务的推定依据，减少企业重复审计成本。 • 认证实施规则。认证原则上自愿，成员国或欧盟委员会可出台法规，要求能源、金融等特定行业强制采用对应认证方案；评估仅覆盖技术风险，不核查供应商地缘、国别相关非技术风险，独立于供应链安全框架评估。	
10	安全隐私验证（NIS2 第 24 条）	**在网络与产品安全方面，NIS2对不同主体提出投用后常态化安全管控要求，分两类明确管控事项。** • 基本实体、重要实体运营阶段需持续落实十项安全举措：风险研判、安全事件监测处置、业务连续性演练、供应链动态核查、漏洞闭环管理、安全措施效能评估、人员安全培训、密码技术落地、人员安全管理、多因素认证与安全通信运维。 • 数字化产品制造商额外执行专项安全管理：维护软件物料清单、及时修复安全漏洞、常态化安全测试、落实协同漏洞披露，搭建完整安全事件处置流程。	出海后
11	外部沟通（报告与记录）（GDPR 第 33‑34 条 AI Act 第 79 条 NIS2 第 23 条（含第 23 条第 4 款、第 29 条、第 31 条） CRA 第 14 条	**在数据合规隐私保护方面，欧盟要求当发生个人数据泄露事件，数据控制者在知悉泄露情况后应立即向监管机构通报。** 通报时限原则上不得超过 72 小时；若超出 72 小时完成报送，需同步书面说明延迟报送的客观原因。经判定泄露行为基本不会对自然人权利与自由构成风险的，可免除向监管机构通报义务。 • 若数据泄露存在侵害自然人权利与自由的高风险，控制者还需及时告知相关数据主体，清晰说明泄露类型、潜在影响以及已落地的风险缓释举措； • 数据处理者一旦发现数据泄露，须第一时间告知对应数据控制者。	出海后
		在AI系统合规方面，欧盟要求明确高风险AI系统事件上报与持续监测义务。 • 高风险 AI 系统服务商若发生或预判将发生致死、重度人身伤害、严重不可逆侵害公民基本权利等重大安全事件，需在 15 日内向市场监管机构提交专项报告。报告需清晰载明事件类型、波及范围及已实施的整改处置方案。 • 企业需搭建上线后常态化监测机制，持续采集、研判 AI 系统实际运行数据，实现风险早识别早处置。	出海后

 版权所有 © 华为云计算技术有限公司

序号	合规重点	适用的具体要求	出海阶段
	CSA 2.0（勒索软件报告义务）第 1 条第 8 款 NIS2 修订草案新增第 23 条第 12、13 款）	• 综上，服务商需同步落实重大事件限时报备与全周期运行监测两项硬性合规要求。	
		在网络与产品安全方面， **1、当基本实体、重要实体遭遇重大网络安全事件时，需执行分阶段限时上报机制。** • 事发 24 小时内向本国 CSIRT 或监管机构报送早期预警，载明事件情况、初步定性、恶意属性与跨境影响； • 72 小时内提交完整详细通报，补充事件信息、影响初步评估及相关入侵指标； • 事件处置完成后 1 个月内出具最终报告，完整说明事件全貌、根因、风险缓释方案及跨境影响。 若安全事件持续发酵，各时限节点可先行报送阶段性进展报告，待事件处置收尾后再按时提交最终报告。企业向监管机构同步威胁情报，不得以商业秘密为借口隐匿必要信息。 **2、数字产品制造商具有漏洞与重大安全事件的分级上报合规义务，要求企业建立完备的内部响应机制，严格落实限时通报要求。** 制造商一旦发现数字产品存在已被恶意利用的漏洞，或发生破坏产品保密性、完整性、可用性的严重安全事件，须通过 ENISA 统一报告平台，同步告知主营地所在成员国 CSIRT 及 ENISA 机构。 上报工作实行分阶段时限管理：事发 24 小时内提交早期预警，72 小时内完成完整漏洞及事件通报，漏洞修复方案落地后 14 天内、安全事件通报后 1 个月内提交最终报告。同时，制造商需搭建标准化的内部漏洞处置与事件响应流程，保障预警上报时效合规。 **3、企业需遵守勒索软件事件专项报送要求，并明确企业前置合规准备义务。** 一是企业发生勒索软件重大网络安全事件，完成常规分阶段上报的基础上，若本国 CSIRT 或主管机构提出要求，需额外报送勒索相关信息，涵盖勒索通知情况、赎金数额、支付渠道、加密钱包地址等内容； 二是企业需健全事件处置与取证流程，提前梳理、落实各类事件上报合规要求。	出海后

 版权所有 © 华为云计算技术有限公司

6 华为云如何遵从及协助客户满足欧洲安全合规要求

中资企业出海欧盟，需遵循以 GDPR、AI Act、CRA、NIS2 及《网络安全法案 2.0》草案构成的五大核心法规体系。在数据合规隐私保护、AI 系统合规、网络与产品安全方面，客户需分阶段落实合规义务：出海前，做好安全治理与能力建设；出海中，管控产品交付与供应链安全；出海后，保障稳定运营与外部沟通。

中资企业在遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

6.1 出海前，建立安全治理体系

合规重点	重点要求描述	客户	华为云
1. 安全治理与管理	在数据合规隐私保护方面，欧盟要求明确数据控制者的合规问责义务，划定数据保护官（DPO）强制设立场景、岗位职责与独立履职保障要求。	a) **客户应依法设立数据保护官（DPO）**：当涉及公共机构处理数据、实施大规模监控行为、或大规模处理健康、生物识别等特殊类别数据时，须强制设立DPO。 b) **保障DPO职责与独立性**：DPO须承担合规指引、内部监督、数据保护影响评估专业建议及对接监管机构与数据主体等核心职能。企业须保障其独立履职，不得施加不合理指令，并为其配置充足的人力、技术与资金资源。 **c) 落实合规问责义务并留存证据**：数据控制者须建立配套管理机制，确	华为云已通过ISO 27001、ISO 27018等国际认证并每年接受第三方审计，客户可获取审计报告作为合规证明材料。 华为云作为账号数据的控制者，在客户与华为云互动过程中，客户向华为云提交账号数据，华为云决定了账号数据的收集方式及处理目的，因此华为云承担数据控制者角色。华为云也将基于PDPL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请求。 华为云作为客户数据的处理者，客户拥有并完全控制客户数据，客户选择以及使用华为云服务存储和处理客户数据，客户通过云服务提供的功能配置或API接口等方式下达指示，华为云按照客户下达的指示处理数据，当

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
		保全部数据处理活动符合GDPR规范，并留存合规证明材料以证明自身履责状态。	客户是客户数据控制者角色时，华为云承担客户数据处理者角色。当客户是客户数据处理者角色时，华为云承担客户数据子处理者角色。 华为云承诺不碰客户数据，并建立安全事件管理与客户通知流程，支撑DPO对外沟通与通报义务
	在AI系统合规方面，AI法案对高风险AI系统提供者提出全流程质量管理体系建设要求，明确体系建设主体、必备合规模块及体系融合规则。	**客户的高风险人工智能系统的提供者需由管理层主导，建立覆盖产品设计、开发、部署全流程的质量管理体系，并确保其持续改进。** 该体系必须完整纳入AI法案的各项合规要求，具体包括：制定合规策略、开展风险管理、实施数据治理、编写技术文档、留存必要记录，以及建立投入使用后的持续监测与事件报告机制。此体系可与现有的ISO 9001等管理体系进行整合，但前提是必须充分满足AI法案的专项合规要求，不得因整合而削弱其合规效力。	华为云提供持续监控与事件响应机制：华为云建立了集中的日志分析系统用于实时监控，并制定了安全事件响应与客户通知流程。客户可依赖此能力满足“投用后持续监测及事件报告”的要求。 华为云可提供数据全生命周期安全服务，支撑数据治理：华为云提供覆盖数据创建、存储、使用、传输、销毁等阶段的安全服务，包括**密码安全中心（Data Encryption Workshop，简称DEW）**及**数据安全中心（Data Security Center，简称DSC）**等工具。这些服务可直接支撑体系中的“数据治理”要求。
	在网络与产品安全方面，欧盟要求 1、明确基本实体与重要实体管理层的网络安全管理职责、法律责任、惩戒机制及能力建设要求。 2、明确制造商管理层的产品合规最终责任，落实管理层在符合性声明、产品管控、体系运维方面的核心职责。	客户的管理层应对网络安全与产品合规承担责任，具体体现在以下三个维度： a) **管理层个人法律责任：**董事会与高管层须亲自审批网络安全风险管控措施并监督落地执行，若发生严重违规，管理层个人将被追究法律责任，甚至面临临时撤销任职资格的惩戒。管理层还须定期参加网络安全专项培训，具备风险评估与业务影响研判能力，将网络安全纳入企业整体战略。	华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并每年接受第三方审计。客户管理层可依据这些审计报告，证明其云上资产运行于经认证的安全基线之上，辅助其履行监督职责。 若客户产品部署于华为云，华为云负责基础设施安全，并已通过ISO27001、SOC等认证这些认证与文档可作为客户产品技术文档中底层环境安全的支撑材料，简化其签署符合性声明前的验证工作。 华为云会安排专人积极配合客户发起的审计和监管机构指定的审计，并可

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
	3、明确企业管理层供应链风险监督职责，划定治理落地与资源保障相关要求。	b) **管理层产品合规最终责任：**制造商管理层须秉持审慎原则，对产品全面符合CRA要求承担最终责任，确保技术文档完整、安全更新及时交付。管理层须对欧盟符合性声明的真实性负责并完成签字确认，同时建立并常态化运维符合规范的质量管理体系与漏洞处置流程。 c) **管理层供应链安全监督责任：**管理层须将供应链映射与高风险供应商排查纳入企业治理体系，全面监督供应链风险，并保障相应的资源投入，确保供应链安全管控措施切实落地。	通过协议约定审计和监督权益，支持客户履行其供应链监督职责。
2 风险管理	在数据合规隐私保护方面，欧盟要求若数据处理活动会对自然人权利与自由形成高风险，数据控制者必须在开展处理工作前完成数据保护影响评估（DPIA）。	**当处理活动因使用新技术而对自然人权利与自由产生高风险时，客户作为数据控制者需在处理前完成数据保护影响评估（DPIA）。** 评估须包含四项内容：系统描述处理操作、分析处理目的与必要性、评估对数据主体权益的风险等级、并制定相应的风险缓释措施。当涉及对个人进行大规模自动化画像、大规模处理健康或生物识别等特殊类别数据、或在大型公共区域进行系统监控时，DPIA为强制性义务。	华为云清晰界定了与客户的责任共担模型，并通过《华为云用户协议》以及《华为云服务等级协议》等文档明确双方安全职责。客户可引用这些认证与文档，作为DPIA中“处理活动描述”及“处理行为合规性与必要性分析”的支撑材料，清晰说明云基础设施的安全水平与数据处理边界。 华为云在《华为云用户协议》中明确表明不会访问或使用用户内容数据，除非是为提供必要服务或遵守法律法规的约束性命令。同时，华为云制定了完善的安全事件管理与客户通知通报流程，当发生安全事件时能及时通知客户。这些承诺与机制可纳入DPIA的风险评估与缓释措施部分，帮助证明数据处理者具备可靠的履约能力与安全保障。

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
	在网络安全合规方面，欧盟要求： 1、核心实体与重要实体应采用适配、均衡的技术、运维及组织管控手段管控网络安全风险。 2、搭载数字功能产品的生产厂商，需在产品设计研发阶段结合已识别风险同步开展安全内置设计，产品上市前完成覆盖用途、使用场景、运行环境、核心资产及全生命周期的网络安全风险评估，相关评估资料统一归档留存。	a) **客户应落实十大安全管控措施：**围绕风险分析、事件处置、业务连续性、供应链安全、系统全生命周期安全、措施有效性评审、网络安全培训、加密管理、人员与访问控制、多因素认证与应急通信等维度，建立适配的技术、运维及组织管控手段。 b) **履行产品上市前置合规义务：**设计阶段嵌入安全内置，上市前完成网络安全风险评估并消除已知漏洞，全面落实安全默认配置、权限管控、数据加密、完整性保护、数据最小化、可用性保障及操作审计追溯。 c) **建立上市后全生命周期管控机制：**常态化管理SBOM清单，持续修复漏洞并开展安全检测，严格执行漏洞披露规范，建立健全安全事件处置体系。	提供安全的开发工具链与基线配置，支撑产品上市前置合规 华为云遵循DevSecOps流程，在开发阶段集成安全开发生命周期（SDL），所有服务发布前须完成静态代码扫描告警清零和多轮安全测试。华为云对操作系统、虚拟机、数据库等均进行安全配置加固，并提供安装安全补丁的公共镜像供客户选用。客户可基于此安全基线和工具链，完成产品设计阶段的安全内置、已知漏洞消除及安全默认配置落实，满足上市前合规要求。 华为云在风险管理方面：每年开展风险评估并在重大变更时增加评估频次；事件处置方面，制定了完善的安全事件响应计划与客户通知通报流程；在业务连续性方面，已通过ISO 22301认证并定期开展应急演练；在供应链安全方面，建立了供应商管理体系，对供应商进行准入尽职调查与年度安全稽查；在访问控制方面，通过**统一身份认证服务（Identity and Access Management，简称IAM）**服务支持多因子认证与细粒度授权；在加密管理方面，提供**密码安全中心（Data Encryption Workshop，简称DEW）**及硬件安全模块；在安全意识方面，建立了覆盖入职、在岗、晋升等环节的培训体系。

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
3. 数据安全与隐私保护	在数据合规隐私保护方面，欧盟要求: 1、数据控制者与处理者落实适配的技术与组织安全措施，明确措施范畴与安全水平的判定依据，保障个人数据全流程安全。 2、规定个人数据处理的基础准则、合法依据、特殊数据管控、数据主体权利及隐私告知规范。 3、明确个人数据跨境传输的合规路径、使用限制、前置义务与禁止条款。	a) 数据控制者与数据处理者须根据数据处理的性质、范围、成本与技术水平，采取包括假名化与加密在内的技术与组织措施，以**保障处理系统的保密性、完整性、可用性和韧性，并确保故障后可恢复**。同时，须建立定期测试与评估措施有效性的流程，以证明安全水平持续达标。 b) **遵循数据处理的核心原则与合法基础**：处理个人数据须恪守合法公正透明、目的限制、数据最小化等七项原则，并基于同意、履约、法定义务等六类合法事由之一方可进行。处理特殊类别数据（如健康、生物识别信息）原则上禁止，仅法定例外场景（如明确同意、重大公共利益）方可行。企业须向数据主体提供清晰易懂的隐私声明，并保障其访问、更正、删除、携带、反对等权利，以及拒绝不受人工干预的自动化决策权。 c) **遵守跨境数据传输的严格规则**：向欧盟境外传输数据，需事先评估第三国保护水平并留存记录，且仅能依托充分性认定、标准合同条款等法定机制之一进行。特殊例外场景仅限个例。企业不得通过数据层层流转的方式规避 GDPR 的保护要求。	华为云在数据存储方面，云硬盘、对象存储、镜像服务等多个服务均提供服务端加密功能，采用高强度算法加密数据，并集成**密码安全中心（Data Encryption Workshop，简称 DEW）**进行密钥全生命周期集中管理，通过经国际安全认证的硬件安全模块（HSM）防止密钥泄露。在数据传输方面，华为云控制台和 API 均采用加密传输协议（TLS）构建安全通道，并提供**虚拟专用网络（Virtual Private Network，简称 VPN）**、**云专线（Direct Connect，简称 DC）**等服务实现混合云场景的安全传输，满足了 GDPR 对“假名化与加密”的要求。 华为云以区域为单位提供服务，区域即客户内容数据的存储位置，未经授权不跨区域移动客户内容数据。客户可依据就近接入原则及适用的法律法规要求自主选择数据存储区域。华为云基础设施采用全球多区域和多可用区模式，各可用区物理隔离。帮助客户落实数据驻留策略，并为其在采用标准合同条款等机制进行跨境传输时，提供关于数据处理地点与安全保障的支撑。 华为云在用户协议中明确表明不会访问或使用用户内容数据，除非是为提供必要服务或遵守法律法规的约束性命令。华为云各服务从设计之初即规划并实现了隔离机制，避免客户间非授权访问，降低数据泄露风险。这为客户履行数据最小化、完整保密等原则，以及向数据主体说明数据处理情况提供了坚实的合约与技术基础。 华为云制定了完善的安全事件管理与客户通知通报流程，分析事件影响并必要时通知客户，内容包括事件描述、影响及建议措施等。同时，华为云提供多粒度数据备份归档服务，客户可对云上文档、硬盘、服务器进行备份，并通过多地域多可用区架构实现容灾，确保故障后数据可恢复。这为客户满足 GDPR 的“可用性与韧

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
			性”、“故障后数据恢复能力”及事件报告要求提供了保障。 华为云提供**数据安全中心（Data Security Center，简称DSC）**，支持数据分类分级、数据水印溯源、数据脱敏等能力，帮助客户高效管理数据。同时，华为云明确其作为数据处理者的角色，按客户指示处理数据，响应数据主体的访问、更正、删除、携带等权利请求提供了技术手段和清晰的责任角色界定。
	在AI系统合规方面，欧盟要求高风险AI 系统在全生命周期内保持合规的准确性、鲁棒性与网络安全水平，明确各维度落地标准。	a) 客户作为高风险AI系统的提供者应确保系统在全生命周期内持续满足准确性、鲁棒性与网络安全的合规要求。 b) 在准确性层面，需在技术文档中明确载明系统在预期用途下的准确性指标。在鲁棒性与网络安全层面，系统需具备抵御运行错误、误用及对抗性攻击的能力，并配置与风险等级相匹配的防护机制，以有效防范模型反演、对抗样本、数据投毒等AI专项攻击。	华为云可提供覆盖AI开发全流程的平台工具，支撑准确性与鲁棒性验证。华为云 **ModelArts** 提供数据标注、模型训练、模型评估、模型部署等 AI 开发全流程服务。其中模型评估模块支持对模型进行精度评估，可输出准确率、精确率、召回率等指标，帮助客户在技术文档中载明系统在预期用途下的准确性指标。同时，ModelArts 支持对模型的安全性和鲁棒性进行扫描检测，帮助客户识别模型潜在风险。 华为云 ModelArts 提供模型安全检测功能，可对模型进行对抗样本攻击检测、模型后门检测等安全评估，帮助客户识别模型在面对对抗性攻击时的脆弱性。此类检测能力直接对应 AI 法案要求的“防范对抗样本、数据投毒等 AI 专项攻击”，为客户配置与风险等级匹配的防护机制提供技术手段。
	在网络与产品安全方面，欧盟要求 1、基本实体与重要实体落实十大类体系化安全管控措施，筑牢网络安全防护屏障。 2、欧盟对带有数字元素的产品明确全维度安全合规要求，由制造商负责	a) 基本实体与重要实体须围绕多因素认证、加密技术、访问控制、业务连续性管理、备份恢复、人员安全及网络安全培训等核心维度，建立体系化的安全管控措施。具体须采用强加密算法保护数据，严格落实最小权限原则，定期备份数据并测试恢复流	在访问控制方面，客户可使用华为云**统一身份认证服务（Identity and Access Management，简称IAM）**支持多因子认证、细粒度授权及访问控制列表设置，助力客户落实最小权限原则。在加密方面，华为云**密码安全中心（Data Encryption Workshop，简称DEW）**使用经国际安全认证的硬件安全模块（HSM）管理密钥，云硬盘、对象存储等多个服务均支持服务端加密。在业务连续性与备份恢复方

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
	落实，覆盖产品技术防护与数据全生命周期管理两大层面。 3、欧盟对带有数字元素产品的制造商明确产品支持周期与安全更新管理规则，保障产品全生命周期持续满足安全合规要求。	程，制定业务连续性与灾难恢复计划，并面向全员开展涵盖钓鱼邮件识别等内容的网络安全培训。 b) 制造商须在设计阶段即融入网络安全原则，出厂默认禁用不安全协议与非必要服务；通过认证机制落实访问控制，采取冗余设计及 DDoS 防护保障可用性，并通过关闭冗余端口、部署 ASLR/DEP 等防护手段压缩攻击面、缓解漏洞风险。同时须同步记录关键安全事件日志，保障日志的机密性与完整性。 c) 采用行业认可的加密算法保护静态与传输中的数据，通过数字签名、哈希校验防范数据篡改；严格遵循数据最小化原则，仅收集实现目的所必需的数据并向用户明示收集范围与用途。产品须支持安全数据删除功能，确保已删除数据不可恢复，并保障跨系统数据传输全程加密与完整性保护。 d) 产品支持期自上市起不得少于 5 年，需上市前确定并在用户说明中标注起止时间及期满风险。支持期内需免费持续推送安全更新以修复漏洞，且安全更新须与功能更新明确区分。安全更新发布后须按“至	面，华为云提供**云硬盘备份（Volume Backup Service，简称VBS）**、**云服务器备份（Cloud Server Backup Service，简称CSBS）**等多粒度备份服务，并基于多地域多可用区架构支持客户构建灾备方。华为云已通过ISO 22301业务连续性管理体系认证，每年定期开展应急演练与测。 华为云在数据存储方面，云硬盘、对象存储等服务提供服务端加密功能，采用高强度算法加密数据。在数据传输方面，控制台和API均采用加密传输协议（TLS）构建安全通道，并支持**虚拟专用网络（Virtual Private Network，简称VPN）**、**云专线（Direct Connect，简称DC）**等服务实现混合云安全传输。在数据销毁方面，客户确认删除后，华为云先删除数据索引关系，并对存储空间进行清零操作，确保数据不可恢复；物理介质报废则通过消磁、折弯或破碎方式清除数据。满足法规“安全数据删除”与“传输全程加密”的要求。 华为云建立了集中、完整的日志大数据分析系统，统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志及告警日志，具备海量日志快速收集、处理、实时分析能力，所有日志保存时间超过180天，90天内可实时查询，并支持与第三方SIEM系统对接。**云审计服务（Cloud TraceService，简称CTS）**可提供对各种云资源操作记录的收集、存储和查询功能，支撑安全分析、合规审计等场景。

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
		少 10 年或支持期剩余时长”的较长期限留存归档。若未按要求推送安全更新，产品可被要求下架。	
4 人员与意识	在 AI 系统合规方面，欧盟要求AI系统提供者与部署者明确人员AI素养建设义务，区分通用建设要求、高风险系统专项责任与供给方支撑义务，确保人员能力匹配岗位需求与系统风险等级。	a) AI系统提供者与部署者均需为开发、使用、监督及管理AI系统的全链条人员制定适配的素养提升措施，内容须结合人员技术背景、应用场景及系统风险等级，并随技术迭代持续更新。 b) 高风险统部署者需承担专项责任，需要确保操作人员具备准确理解系统输出、及时识别误用或故障、有效履行人类监督职责的能力。 c) AI系统提供者须向部署者交付必要的培训材料与相关信息，支撑其内部AI素养建设落地。	华为云提供丰富的产品文档、最佳实践指南及安全配置建议，帮助客户理解AI系统的功能特性、安全能力及使用规范。客户可据此制定操作人员的专项培训材料，确保其能准确理解系统输出、识别误用或故障，满足高风险AI系统部署者的专项责任要求。 华为云设置专门负责安全及隐私保护的角色，配备专业安全事件响应团队及专家资源池，并建立了成熟的漏洞响应与安全运维机制。客户可借助华为云的安全专业知识与服务，持续获取最新安全实践，确保自身AI素养措施随技术迭代持续更新。

6.2 出海中，管控产品交付与供应链安全

合规重点	重点要求描述	客户	华为云
5 开发与部署	在网络与产品安全方面，欧盟要求 1、对数字产品	a) 客户应编制全流程技术文档，需覆盖设计、开发、生产、投用全阶段的技术文档，内容须包含网络安全风险评估、	华为云遵循DevSecOps流程，集成安全开发生命周期（SDL），覆盖安全需求分析、安全设计、安全编码和测试、安全验收和发布、漏洞管理等环节，所有云服务发布前均须完成多轮安全测试与静

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
	制造商设置全流程文档编制、用户安全告知及长期留存义务，强化产品全生命周期安全可追溯性。 2、法规对数字产品制造商设置全流程文档编制、用户安全告知及长期留存义务，强化产品全生命周期安全可追溯性。	软件物料清单（SBOM）、安全测试审查结果及漏洞处理流程记录。 b) 提供通俗化用户使用说明，编写面向用户的说明文档，列明产品预期用途、安全功能、厂商信息、服务支持周期、安全更新与配置指引及漏洞报送渠道。 c) 履行长期留存义务，技术文档与欧盟符合性声明副本，须自最后一件产品投放市场起留存至少10年，以备监管机构调阅核查。	态代码扫描告警清零。客户可基于此工具链产出的安全测试记录、漏洞处理记录等材料，作为编制全流程技术文档的核心支撑。 华为云每年至少进行一次正式风险评估，识别威胁与漏洞并制定风险处置计划。同时，华为云建立了完善的安全事件管理与漏洞响应机制，确保漏洞在SLA时限内修复并留存处置记录。客户可引用华为云基础设施的安全风险评估结果与漏洞管理记录，作为其产品技术文档中网络安全风险评估、软件物料清单及漏洞处理流程的补充材料。
6 交付和运维	在数据合规隐私保护方面，欧盟要求对个人数据处理活动记录作出明确规范，区分控制者与处理者设置差异化留存要求，并配套相应豁免规则。	a) 客户若是数据控制者需完整留存处理活动记录：数据控制者须以书面或电子形式记录主体身份与联系方式、处理目的、数据及主体类别、接收方范围、跨境传输保障措施、数据留存期限，以及所采取的技术与组织安全措施概述。 b) 客户若是数据处理者需留存受托处理活动记录：数据处理者记录内容与控制者基本一致，但无需载明处理目的，仅需记录所执行的各项处理活动类别。 c) 豁免规则的适用条件：雇员不足250人的企业原则上可豁免记录义务，但若涉及可能侵害	华为云作为账号数据的控制者，在客户与华为云互动过程中，客户向华为云提交账号数据，华为云决定了账号数据的收集方式及处理目的，因此华为云承担数据控制者角色。华为云也将基于PDPL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请求。 华为云作为客户数据的处理者，客户拥有并完全控制客户数据，客户选择以及使用华为云服务存储和处理客户数据，客户通过云服务提供的功能配置或API接口等方式下达指示，华为云按照客户下达的指示处理数据，当客户是客户数据控制者角色时，华为云承担客户数据处理者角色。当客户是客户数据处理者角色时，华为云承担客户数据子处理者角色。

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
		数据主体权利的处理、非偶发性处理，或处理特殊类别数据、刑事定罪相关数据的，仍须履行记录义务。	
	在AI系统合规方面，欧盟要求对高风险 AI 系统构建全生命周期合规监管体系，覆盖入市合规自证、运行追溯管控与监管备案登记全流程。	a) **客户应编制并持续更新技术文档：**高风险AI系统提供者须在投放市场前完成技术文档，涵盖系统概况、预期用途、风险管理体系、研发数据与方法、验证测试结果、准确性指标及网络安全措施，用以自证全面合规。 b) **保障系统可追溯性：**系统须具备自动日志记录功能，完整留存风险事件与系统重大变更等信息，留存时长须与系统预期用途相匹配。 c) **完成欧盟监管数据库注册：**提供者须在欧盟高风险AI系统数据库中提交主体信息、系统说明、符合性声明及第三方认证机构信息（如有）等材料。	华为云**ModelArts**提供从数据标注、模型训练、模型评估到模型部署的全流程服务。其中模型评估模块可输出准确率、精确率、召回率等指标，帮助客户编制技术文档中所需的“准确性指标”与“验证测试结果”。 华为云**ModelArts**支持模型可信评估，可对模型的安全性进行扫描检测，识别潜在风险。提供模型安全检测功能，可对模型进行对抗样本攻击检测、模型后门检测等安全评估。客户可将这些检测结果纳入技术文档的“风险管理体系”章节。

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
	在网络与产品安全方面，欧盟要求 1、对基本实体与重要实体明确网络安全文档留存要求，确保风险管理与事件处置全程可追溯、可核验。 2、法规明确企业供应链映射记录的留存与动态管理要求，支撑监管层面的审计与风险评估工作。 3、法规对进口商、分销商两类流通主体设定全流程合规管控义务，明确入市核验、文档留存与异常处置要求，保障上市产品符合监管标准。	a) **客户应落实网络安全文档留存义务：**基本实体与重要实体须留存风险管理措施落地文档及网络安全事件调查报告，保存期限依成员国法律规定（通常1至5年），文档须能佐证合规执行情况，并在事件场景下向监管机构提供完整调查材料以供审查。 b) **建立供应链映射记录并动态更新：**企业须留存供应链映射记录，涵盖ICT组件来源国、供应商所有权结构、关键资产依赖关系、单一供应商依赖程度及替代供应商可用性等信息，并配合监管审计与风险评估，在供应商或合同状态变更时及时更新。 c) **履行进口商与分销商的合规管控职责：**进口商须核查第三国产品符合性评估、技术文档齐备性及CE标志加贴情况，标注自身信息并留存文档10年，不合规产品禁止上市并通报相关方。分销商须确认产品带有CE标志及全套合规文档，发现不合规产品禁止上市并通知制造商与进口商，知悉严重安全问题时及时告知相关方并配合落实纠正措施。	华为云建立了集中、完整的日志大数据分析系统，统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志及告警日志，具备海量日志快速收集、处理、实时分析能力，所有日志保存时间超过180天，90天内可实时查询，并支持与第三方SIEM系统对接。**云审计服务（Cloud TraceService，简称CTS）**可提供对各种云资源操作记录的收集、存储和查询功能，支撑安全分析、合规审计等场景。客户可依赖此日志留存与审计能力，落实风险管理措施落地文档及安全事件调查记录的长周期保存，满足监管调阅要求。 华为云在供应链安全管理方面，公开披露自身财务状况、声誉、技术能力、运营体系等信息。客户可将华为云作为关键ICT供应商的相关信息纳入供应链映射记录，覆盖供应商所有权结构、依赖程度及替代供应商可用性等内容，并配合监管审计工作。 华为云制定了完善的事件管理和客户通知通报流程，当底层基础平台发生安全事件并可能影响客户时，将启动通知通报机制，将事件描述、起因、影响、已采取措施及建议客户采取的措施等内容通知客户。客户可依赖此机制，在知悉产品存在严重安全问题时，及时获取相关信息并向监管机构及下游方通报，配合落实纠正措施。 华为云通过**《华为云用户协议》**以及**《华为云服务等级协议》**，明确规定了所提供服务的内容、服务水平及双方安全职责划分。客户可依据这些协议，清晰界定自身作为进口商或分销商在产品安全合规管控中的责任范围，并为监管审计提供责任边界的书面证据。

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
7 供应链管理	在数据合规隐私保护方面，法规对数据控制者委托第三方处理数据作出完整约束，明确双方权责、协议规范与持续管控要求。	**数据控制者委托第三方处理个人数据时，需严格履行选任、约束与持续监督三项义务。** a) 首先，仅可选择具备充分技术能力与可靠性的处理者，并与之签署书面数据处理协议，明确约定处理的范围、周期、目的，以及所涉个人数据与数据主体的类型。 b) 其次，须通过协议确保处理者仅按控制者的书面指令操作，落实必要的安全防护措施，协助控制者响应数据主体的权利请求，并在合同终止后返还或彻底清除所有个人数据。 c) 最后，控制者须定期核查处理者的安全合规状况，而处理者未经控制者书面明确许可，不得擅自引入次级处理者。	华为云作为账号数据的控制者，在客户与华为云互动过程中，客户向华为云提交账号数据，华为云决定了账号数据的收集方式及处理目的，因此华为云承担数据控制者角色。华为云也将基于PDPL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请求。 华为云作为客户数据的处理者，客户拥有并完全控制客户数据，客户选择以及使用华为云服务存储和处理客户数据，客户通过云服务提供的功能配置或API接口等方式下达指示，华为云按照客户下达的指示处理数据，当客户是客户数据控制者角色时，华为云承担客户数据处理者角色。当客户是客户数据处理者角色时，华为云承担客户数据子处理者角色。
	在AI系统合规方面，高风险 AI 系统数据集管控及通用 AI 模型信息披露两项合规要求。	a) 客户若是高风险AI系统的服务商，需对训练、验证及测试数据集实施全流程规范管理，重点核查数据的来源合规性、采集方式、标注质量及潜在偏见，并主动管控偏见风险，确保模型输出不会产生歧视性后果。 b) 通用AI模型的供应方须向下游使用者提供充分透明的信息，包括模型名称、版本、能力说明、使用约束条件及训练数据概要等，以保障下游主体能够据此履行	华为云**ModelArts**提供数据标注、模型训练、模型评估、模型部署等AI开发全流程服务。其中模型评估模块支持对模型进行精度评估，可输出准确率、精确率、召回率等指标，帮助客户在技术文档中载明系统在预期用途下的准确性指标。同时，ModelArts支持对模型的安全性和鲁棒性进行扫描检测，帮助客户识别模型潜在风险。 华为云**ModelArts**提供模型安全检测功能，可对模型进行对抗样本攻击检测、模型后门检测等安全评估，帮助客户识别模型在面对对抗性攻击时的脆弱性。此类检测能力直接对应AI法案要求的“防范对抗样本、数据投毒等AI专项攻击”，为客户配置与风险等级匹配的防

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
		其在《AI法案》下的合规义务。	护机制提供技术手段
	在网络与产品安全方面，欧盟要求 1、建立供应链安全管控机制，明确关键主体管控义务与监管层协同评估机制，实现供应链风险全链路覆盖。 2、明确企业在ICT 供应链风险管控中的两项核心义务，全面支撑欧盟层面的协同监管与风险评估工作。 3、欧盟对企业ICT 供应链设置全链条管控规则，明确映射管理、高风险供应商处置及风险缓释三项合规要求。 4、数字产品制造商建立软件组件全量管理与协	客户应将供应链安全纳入风险管理：将供应链安全纳入整体风控框架，核查供应商安全能力，在采购环节落实风险评估，并持续监控供应商合规状态。 a) **配合欧盟协同评估并建立供应链映射**：配合欧盟开展ICT供应链安全风险评估，按要求提供信息；同时建立映射制度，记录组件来源国、供应商所有权结构及单一依赖风险。 b) **处置高风险供应商并推动多元化**：供应商一旦被列入高风险清单，须立即停止新采购及合同延期，按期拆除替换高风险组件，并制定供应商多元化策略以降低中断风险。 c) **建立SBOM与漏洞披露机制**：制造商须编制软件物料清单（SBOM），覆盖全部组件、版本及依赖关系；同时建立协同漏洞	华为云建立了集中、完整的日志大数据分析系统，统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志及告警日志，具备海量日志快速收集、处理、实时分析能力，所有日志保存时间超过180天，90天内可实时查询，并支持与第三方SIEM系统对接。**云审计服务（Cloud TraceService，简称CTS）**可提供对各种云资源操作记录的收集、存储和查询功能，支撑安全分析、合规审计等场景。 华为云在供应链安全管理方面，公开披露自身财务状况、声誉、技术能力、运营体系等信息。客户可将华为云作为关键ICT供应商的相关信息纳入供应链映射记录，覆盖供应商所有权结构、依赖程度及替代供应商可用性等内容，并配合监管审计工作。 华为云已通过ISO 27001、ISO 27017、ISO 27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并每年接受第三方审计，可向客户提供相关审计报告与认证证书副本。客户可据此，核查产品符合性评估完成情况与技术文档齐备性，并将其作为符合性声明副本留存的组成部分，满足10年留存义务。

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
	同漏洞披露双重机制，落实产品全生命周期安全管控义务。	披露渠道，及时处置并修复第三方组件漏洞。	
8 AI 安全	在AI安全领域，1、欧盟要求对通用 AI 模型实行分级监管，以风险等级匹配差异化合规义务，系统性风险模型适用更为严格的管控要求。 2、欧盟要求高风险AI系统提供者搭建、落地、留存文档并持续运维覆盖 AI 全生命周期的风险管理体系。	a) **客户应识别是否属于系统性风险模型并履行通报义务**：通用AI模型提供者须根据技术评估、欧盟委员会认定或训练计算量超过10^{25}次浮点运算等标准，判断是否属于系统性风险模型。若达标，须在两周内向欧盟委员会通报，并可举证抗辩以排除认定。 b) **所有通用AI模型均须履行基础合规义务**：包括编制并动态更新技术文档，向产业链下游提供模型信息与使用约束，制定欧盟版权合规使用政策，以及公开发布训练内容摘要。 c) **系统性风险模型须承担额外管控义务**：须开展覆盖网络攻击、偏见、有害内容等风险的全生命周期评估与缓释，建立严重事件上报机制，并落实高水平网络安全防护，防范权重泄露、对抗性攻击等安全风险。	华为云建立了集中、完整的日志大数据分析系统，统一收集各层管理行为日志及威胁检测告警日志，所有日志保存时间超过180天，90天内可实时查询。同时，华为云制定了完善的安全事件管理与客户通知通报流程，当发生安全事件时可及时通知客户。客户可依赖此能力，落实高风险AI系统上线后的持续监测、新增风险识别及严重事件上报义务。 华为云建立了稳固的多层立体安全防护系统，部署Anti-DDoS、IDS/IPS、WAF等防护机制，可实时检测和阻断来自互联网的网络攻击。华为云使用态势感知分析系统，关联各安全设备告警日志统一分析，快速识别已发生攻击并预判未发生威。在数据加密方面，华为云**密码安全中心（Data Encryption Workshop，简称DEW）**服务通过经国际安全认证的硬件安全模块（HSM）进行密钥管理，防止密钥泄露。这些能力为客户防范权重泄露、对抗性攻击等安全风险提供了多层防护屏障。

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
		d) **高风险AI系统提供者须建立并运维全生命周期风险管理体系**：需识别并评估正常使用及可预见误用情形下的各类风险，结合上线后监测数据补充识别新增风险，配套执行风险处置措施，并定期对风险管理制度进行全面复核与迭代更新。	
9 安全许可与销售	在 AI 安全领域，欧盟对高风险 AI 系统明确入市前符合性评定规则，覆盖评估实施、声明出具与标识加贴全流程，保障系统符合 AI 法案监管要求。	a) **客户应完成入市前符合性评估**：高风险AI系统投放市场前须完成符合性评估。采用协调标准的系统可进行基于内部控制的自我评估；未使用协调标准或涉及极高风险场景的系统，须由通知机构实施第三方评估。 b) **出具欧盟符合性声明**：评估通过后须出具符合性声明，载明提供者信息、系统唯一识别信息、合规声明内容及授权签名，确认系统符合AI法案全部要求。 c) **加贴CE标志**：须在系统本体、包装或随附文件上加贴清晰可见、易于辨认且不可磨灭的CE标志。	华为云**ModelArts**提供数据标注、模型训练、模型评估、模型部署等AI开发全流程服务。其中模型评估模块支持对模型进行精度评估，可输出准确率、精确率、召回率等指标，帮助客户在技术文档中载明系统在预期用途下的准确性指标。同时，ModelArts支持对模型的安全性和鲁棒性进行扫描检测，帮助客户识别模型潜在风险。 华为云**ModelArts**提供模型安全检测功能，可对模型进行对抗样本攻击检测、模型后门检测等安全评估，帮助客户识别模型在面对对抗性攻击时的脆弱性。此类检测能力直接对应AI法案要求的“防范对抗样本、数据投毒等AI专项攻击”，为客户配置与风险等级匹配的防护机制提供技术手段。

 版权所有 © 华为云计算技术有限公司

合规重点	重点要求描述	客户	华为云
	在网络与产品安全方面，欧盟要求 1、对带有数字元素的产品明确入市前符合性评定全流程要求，按产品类别与风险等级实施差异化评估机制，保障产品符合CRA 监管标准。 2、对基本实体和重要实体的合规认证实施可选认证、差异化审查机制，明确ECCF 认证效力，兼容国际通用安全标准。 3、实体级网络安全态势认证面向企业整体安全能力评估，具备合规减负作用，并明确认证性质与评估边界两大核心规则。	客户应按产品类别与风险等级完成入市前符合性评估：一般产品可采取基于内部生产控制的自我评估；重要产品Class I在完全适用协调标准的前提下可自我评估，否则须由通知机构参与评估；重要产品Class II及关键产品强制要求通知机构参与评估。	华为云已通过ISO 27001、ISO 27017、ISO 27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并每年接受第三方审计，可向客户提供审计报告与认证证书副本。客户可引用华为云基础设施的合规认证，作为自我评估的支撑材料，或作为通知机构参与评估时的合规佐证。

 版权所有 © 华为云计算技术有限公司

6.3 出海后，保障稳定运营与外部沟通

合规重点	重点要求描述	客户	华为云
10 安全隐私验证	在网络与产品安全方面，NIS2对投用后阶段提出两类常态化安全管控要求：基本实体与重要实体须落实十项安全运营举措，数字化产品制造商须额外执行产品专项安全管理。	a) **客户作为基本实体与重要实体需落实十项常态化安全举措：**运营阶段须持续开展风险研判、安全事件监测处置、业务连续性演练、供应链动态核查、漏洞闭环管理、安全措施效能评估、人员安全培训、密码技术落地、人员安全管理，以及多因素认证与安全通信运维。 b) **数字化产品制造商须履行专项安全管理义务：**维护软件物料清单（SBOM），及时修复安全漏洞，开展常态化安全测试，落实协同漏洞披露，并搭建完整的安全事件处置流程。	华为云提供常态化安全运营能力，支撑十项举措落地。在风险研判方面，华为云每年至少进行一次正式风险评估，并定期召开风险评估会议。在事件监测处置方面，华为云建立了集中的日志大数据分析系统，实时监控并检测安全事件，同时制定了完善的安全事件响应与客户通知流程。在业务连续性方面，华为云已通过ISO 22301认证，每年定期开展应急演练与测试。在供应链管理方面，华为云建立了供应商管理体系，对供应商进行准入尽职调查与年度安全稽查。在加密管理方面，华为云提供**密码安全中心（Data Encryption Workshop，简称DEW）**，通过经国际安全认证的硬件安全模块（HSM）管理密钥。在访问控制方面，华为云**统一身份认证服务（Identity and Access Management，简称IAM）**支持多因子认证与细粒度授。在安全培训方面，华为云建立了覆盖全员的培训体系与违规问责机制。 华为云已建立成熟的漏洞响应机制，确保自研和第三方漏洞在SLA时限内完成修复，并通过灰度发布或蓝绿部署方式安全交付更新。同时，华为云定期开展内部和第三方渗透测试与安全评估，保障云服务安全性。华为云遵循DevSecOps流程，所有服务发布前须完成多轮安全测试与静态代码扫描告警清零。客户可借助这些漏洞管理、安全测试机制及安全开发实践，履行SBOM维护、漏洞修复、常态化安全测试、协同漏洞披露及安全事件处置等产品专项管理义务。 华为云有专门的审计团队定期评估策略、规程及配套措施的符合性和有效性，并向最高管理层报告调查结果和建

 版权所有 © 华为云计算技术有限公司

			议。同时，华为云每年定期开展风险评估、管理评审等活动，识别体系运行过程中的问题并实施整改，推动管理体系持续改进。
11 外部沟通	在数据合规隐私保护方面，欧盟要求当发生个人数据泄露事件，数据控制者在知悉泄露情况后应立即向监管机构通报。	a) 数据控制者须在72小时内向监管机构通报数据泄露，逾期须书面说明延迟原因；若泄露不会对个人权利与自由构成风险，可免除通报义务。 b) 高风险泄露须及时告知受影响的数据主体，说明泄露类型、潜在影响及已采取的风险缓释措施。 c) 数据处理者发现泄露需第一时间告知对应控制者。	华为云设置7×24小时专业安全事件响应团队及专家资源池，制定了完善的事件管理和客户通知通报流程。当底层基础平台发生安全事件并对客户产生影响时，将启动通知通报机制，向客户通报事件描述、起因、影响、已采取措施及建议客户采取的措施等内容。在底层基础平台发生严重事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快时间内通知客户。事件解决后，会根据具体情况向客户提供事件报告。客户可依赖此机制，及时获取事件信息以完成24小时早期预警、72小时完整通报及最终报告的分阶段上报。 华为云已建立成熟的漏洞响应机制，华为CSIRT和华为云安全运维团队建立了漏洞感知、处置和对外披露的机制，确保自研和第三方漏洞在SLA时间内完成响应和修复。华为云还制定了安全事件定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级。客户可参照此机制，构建自身漏洞分级报告流程，满足24小时早期预警、72小时完整通报及漏洞修复后14天内提交最终报告的时限要求。 华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程并
	在AI系统合规方面，欧盟要求明确高风险AI系统事件上报与持续监测义务。 •	a) 重大安全事件须在15日内向监管机构提交专项报告，载明事件类型、波及范围及已实施的整改处置方案。适用情形包括致死、重度人身伤害、严重不可逆侵害公民基本权利等。 b) 需搭建上线后常态化监测机制，持续采集与分析系统运行数据，实现风险早识别、早处置。	

	在网络与产品安全方面， 1、当基本实体、重要实体遭遇重大网络安全事件时，需执行分阶段限时上报机制。 2、数字产品制造商具有漏洞与重大安全事件的分级上报合规义务，要求企业建立完备的内部响应机制，严格落实限时通报要求。 3、企业需遵守勒索软件事件专项报送要求，并明确企业前置合规准备义务。	a) **重大网络安全事件执行分阶段限时上报**：事发24小时内提交早期预警，72小时内提交完整通报，事件处置完成后1个月内出具最终报告。事件持续发酵时先行报送阶段性进展，不得以商业秘密为由隐匿必要信息。 b) **漏洞与严重安全事件分级上报**：制造商发现已被利用的漏洞或破坏产品安全性的严重事件，须通过ENISA平台告知所在国CSIRT及ENISA。实行分阶段时限管理：24小时内提交早期预警，72小时内完成完整通报，漏洞修复后14天内、事件通报后1个月内提交最终报告。 c) **搭建标准化的内部漏洞处置与事件响应流程**：制造商需建立完备的内部响应机制，保障预警上报时效合规。 d) **勒索软件事件履行专项报送义务**：在完成常规分阶段上报的基础上，若监管机构要求，须额外报送勒索通知情况、赎金数额、支付渠道、加密钱包地址等信息。 e) **健全事件处置与取证流程**：企业须提前梳理并落实各类事件上报合规要求，做好前置合规准备。	持续优化，清晰定义了事件响应过程中各角色的职责。华为云每年对信息安全事件管理程序和流程进行测试，所有安全事件响应人员均需参与。同时，华为云制定了突发事件应急预案，详细规定了应急响应的组织、程序与操作规范，并定期进行测。 华为云建立了集中、完整的日志大数据分析系统，统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志及威胁检测告警日志，所有日志保存时间超过180天，90天内可实时查询，具备海量日志快速收集、处理、实时分析能力。当服务器或应用疑似被入侵时，由安全响应人员进行取证分析，并定期对事件进行统计和趋势分析，找到根本原因并制定解决方案从根源上杜绝该类事件发生。客户可依赖此日志取证与溯源能力，健全事件处置与取证流程，满足勒索软件事件专项报送及各类事件上报的合规要求。

 版权所有 © 华为云计算技术有限公司

7 华为云为客户提供的安全与隐私保护相关的云服务

客户负责客户数据安全，为保障客户内容安全，客户可以根据客户内容适合的安全级别，采取额外的安全措施，额外的安全措施可以来源华为云，也可来源第三方。

华为云理解客户的安全与隐私保护需求，并结合自身丰富安全与隐私保护实践及技术能力，提供了相关的安全与隐私保护相关云服务供客户选择。云服务涵盖网络、数据库、安全、管理与部署工具等产品，相关产品的数据保护、数据删除、网络隔离、权限管理、容灾备份、安全审计等功能可帮助客户加强安全保障。

- **安全合规**

产品名称	产品介绍	核心功能
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。	安全防护
云防火墙 Cloud Firewall (CFW)	CFW是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，让用户快速灵活应对威胁。 云防火墙服务是为用户业务上云提供网络安全防护的基础服务。	资产保护 访问控制 在线防御
企业主机安全 Host Security Service (HSS)	HSS 能提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助企业更方便地管理主机安全风险，实时发现并阻止黑客入侵行为。 客户可通过HSS更方便地管理主机、容器的安全风险，实时发现勒索、挖矿、渗透、逃逸等入侵行为，以满足等保合规的要求。	资产管理 漏洞管理 入侵检测

 版权所有 © 华为云计算技术有限公司

产品名称	产品介绍	核心功能
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。	安全审计
密码安全中心 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。	数据加密
DDoS防护 Anti-DDoS Service (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。	安全防护
数据安全中心 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。 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。	数据分级分类 数据脱敏 数据水印
云堡垒机 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。 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。	权限管理
云证书与管理服务 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。 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	证书管理
安全云脑 SecMaster	安全云脑基于云原生安全，提供全面的日志采集、安全治理、智能分析、态势感知、编排响应等快速闭环的安全信息和事件管理能力，实现自动化安全运营，助客户守护云上安全。	态势感知 安全运营

- **存储**

存储产品名称	产品介绍	核心功能
云备份 Cloud Backup and Recovery (CBR)	CBR为云上的弹性云服务器、裸金属服务器、云硬盘、云下VMware虚拟化环境和本地文件 目录，提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数	数据备份

 版权所有 © 华为云计算技术有限公司

存储产品名称	产品介绍	核心功能
	据恢复到任意备份点。	
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。	数据备份
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。	数据备份

- **管理与监督**

产品名称	产品介绍	核心功能
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)账号，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。	权限管理
云审计服务 Cloud Trace Service (CTS)	为客户提供云账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，保障数据主体的知情权、实现快速查找。	安全审计
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。	安全审计
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保留对个人信息的操作记录，保障数据主体的知情权。	安全审计
配置审计 Config	配置审计(Config)服务提供全局资源配置的检索，配置历史追溯，以及基于资源配置的持续的审计评估能力。 客户可通过Config查看资源详情、资源之间的关系、资源历史，并可以通过配置合规规则来对资	安全审计

 版权所有 © 华为云计算技术有限公司

产品名称	产品介绍	核心功能
	源进行合规性检查，确保云上资源配置变更符合预期。	

- **网络**

产品名称	产品介绍	核心功能
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	安全传输
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。	网络隔离

 版权所有 © 华为云计算技术有限公司

8 结语

华为云致力于为出海欧洲的中资企业提供符合欧盟监管要求的安全、可信的云环境，并持续运营华为云安全保障体系。本文系统梳理了GDPR、AI Act、CRA、NIS2及CSA 2.0草案等核心法规的适用要求，阐述了华为云在数据隐私、网络安全、AI治理等重点领域的安全实践与合规认证，有助于客户深入了解华为云对欧盟监管框架的遵从性，让客户安全、放心地使用华为云。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合欧盟监管要求的安全云环境，明确出海前、出海中、出海后各阶段的责任边界，帮助客户更好地与华为云共同承担起相应的合规与安全责任。

本白皮书仅供参考，不具备任何法律效力或构成任何形式的法律建议。客户应酌情评估自身使用云服务的情况及业务所在欧盟成员国的具体转化立法，并确保在使用华为云时对相关监管要求的遵从性。

 版权所有 © 华为云计算技术有限公司

9 版本历史

日期	版本	描述
2026 年 7 月	1.0	首次发布

 版权所有 © 华为云计算技术有限公司