云计算开源产业联盟
OpenSource Cloud Alliance for industRy,OSCAR

云服务商个人数据保护指南

（2018年）

云计算开源产业联盟

2018年8月

版权声明

编写说明

牵头单位：中国信息通信研究院

参与单位：华为软件技术有限公司、北京京东叁佰陆拾度电子商务有限公司、腾讯云计算（北京）有限责任公司、北京百度网讯科技有限公司、中国电信云计算分公司、上海优刻得信息科技有限公司、北京世纪互联宽带数据中心有限公司、上海蓝云网络科技有限公司、北京中联润通信息技术有限公司、北京迅达云成科技有限公司

编写人： 栗蔚、郭雪、武倩聿、孔松、段晓蓉、白莹婷、宋文娣、严少敏、王永霞、杨俊、康和、潘文君、胡皆欢、樊龙、周行健、陈澍、周明、董伟

目录

前言

当前，云计算服务面临的风险日趋复杂多样，数据安全问题日益凸显。2018 年 5 月 25 日欧盟《一般数据保护条例》正式施行，我国、新加坡、日本等也出台了个人数据保护相关法律法规。从全球范围来看，各国对个人数据保护的要求愈发严格。如何有效保护个人数据安全、满足各国法律法规的监管要求，是云服务商出海面临的共同问题。

《云服务商个人数据保护指南》首先梳理各国个人数据保护相关法律法规以及国内外数据保护相关标准，提出了个人数据保护的六项原则，最后对云服务商在个人数据保护方面可以采取的措施给出了建议。

云服务商个人数据保护指南

一、概述

(一) 个人数据范畴

在大多数情况下，我们对数据获取、传输、处理和使用的任何描述，都要在之前对所涉及的具体数据类别进行清晰的说明。云服务生态系统中涉及多种数据类别，按照 ISO/IEC 19944:2017(E)《信息技术——云计算——云服务和设备：数据流、数据类别和数据使用》的划分主要有四种，分别为：

1）账户数据

通常在云服务用户购买云服务时生成，用于帮助云服务用户管理云服务。账户数据主要由云服务用户提供的数据元素组成，包括：姓名、地址、电话等。

2）云服务用户数据

基于法律或其他方面的原因，由云服务用户所控制的一类数据对象，这些数据对象包括输入到云服务的数据，或云服务用户通过已发布的云服务接口执行云服务所产生的数据。

3）云服务衍生数据

云服务提供者控制下的一类数据对象，由云服务用户与云服务交互产生。包括：日志数据，授权用户数以及授权用户的身份，配置数据和定制化数据。

4）云服务供应商数据

由云服务操作产生，在云服务提供者控制下的一类数据对象。包括：资源配置和利用信息、云服务专用虚拟机、存储和网络资源分配、总体数据中心配置和利用、物理和虚拟资源故障率、操作成本等。

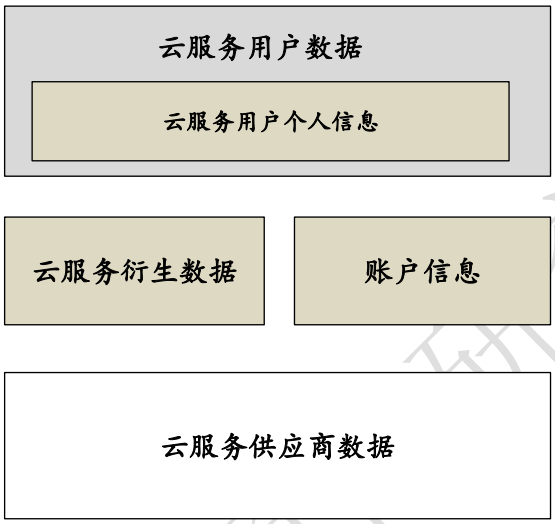


图 1 云服务商个人数据保护的数据范畴示意图

云服务商个人数据保护所涉及的数据范畴主要包括账户数据、云服务衍生数据和云服务用户数据，如图 1 所示。其中，云服务用户数据中可能包含云用户存储于云上的个人信息（如：电商企业将自己的网站部署于云上，用户在网站上的注册信息、收货信息等数据存在云上）。

（二） 云服务商与个人数据的关系

对于云服务商而言，个人数据包括云上用户账户信息、云服务衍生数据以及云服务用户数据，其中云服务用户数据涉及云上用户所服务的终端用户的账户信息和衍生数据。

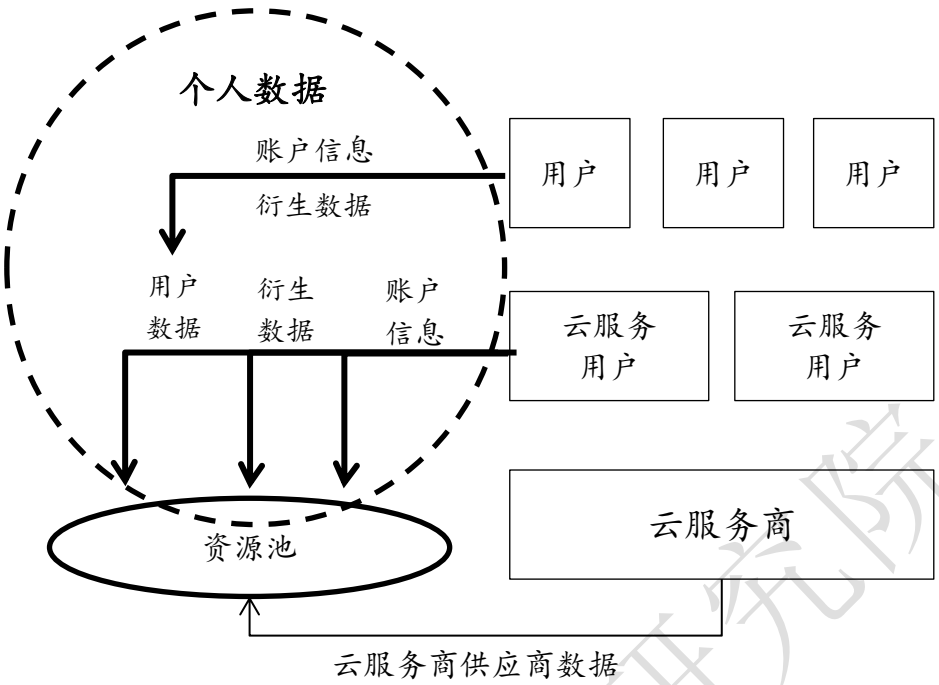


图 2 云服务商与个人数据的关系图

（三） 各国个人数据保护相关法律及云服务商合规要求

1. 中国

我国数据保护方面的法律法规仍处于发展阶段，已有法律主要是从数据处理合法、用户权利、数据安全、事故披露、跨境传输等方面对数据保护进行要求。

《中华人民共和国网络安全法》于 2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过。该法规定了公民个人信息保护的基本法律制度，具体要求可分为六大方面：一是网络运营者收集、使用和处理个人信息必须遵循合法、正当、必要的原则；二是规定网络运营商收集、使用和处理公民个人信息的目的明确原则和知情同意原则；三是网络运营商应确保

个人信息的安全性，在发生或即将发生个人信息安全事件时，应向用户和主管部门告知；四是明确公民个人信息的删除权和更正权制度；五是对个人信息跨境传输提出要求，关键信息基础设施的运营者在境内运营中收集和产生的个人信息和重要数据应当在境内存储。确需向境外提供的，应当按照规定进行安全评估。六是网络安全监督管理机构及其工作人员对公民个人信息、隐私和商业秘密的保密制度等。

《中华人民共和国刑法修正案七》于2009年2月28日正式发布。该法规定，企业在履行职责或提供服务过程中获得的个人数据，如违反国家相关规定，出售或提供给他人且情节严重的，将可能受到刑事处罚。

针对我国《网络安全法》的相关规定，涉及云服务商需要满足的要求主要包括：

a）产品、服务具有收集用户信息功能的，应当向用户明示并取得同意。

b）云服务商应当采取技术措施和其他必要措施，确保公民个人信息安全，防止其收集的公民个人信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施，告知可能受到影响的用户，并按照规定向有关主管部门报告。

c）云服务商应当按照规定留存相关的网络日志不少于六个月。

d）违反《网络安全法》规定，窃取或者以其他方式非法获取、出

售或者非法向他人提供公民个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处五十万元以下罚款。

2. 欧盟

欧盟《一般数据保护条例》（GDPR）明确对数据处理者责任提出了要求，丰富了数据主体的权利，在数据向第三国传输、违规处罚、监管等方面都进行了较为严格的规范。

1）《一般数据保护条例》(GDPR)于 2018 年 5 月 25 日正式生效。GDPR 加强了对欧盟数据主体的权利保护，主要有如下特点：

a）适用范围大。控制者或处理者设立在欧盟、或数据主体为欧盟境内的数据主体，且数据处理行为涉及向该数据主体提供服务或监控其在欧盟的行为，数据处理活动均要满足 GDPR 的要求。

b）修订并增加数据主体的权利。GDPR 修订了《95 指令》中的查阅权、反对权、更正与删除权等权利的内容，增设了限制处理权、数据可携权、被遗忘权。

c）数据控制者和处理者的责任义务加重。GDPR 将数据处理者纳入要求对象，在部分情况下提出了与数据控制者同等的要求，监管机构的监管范围从控制者扩大到处理者。GDPR 要求数据处理应有处理活动记录；控制者应进行数据保护影响评估；个人数据泄露时，控制者应在得知数据泄露事

件后 72 小时内向监管机构报告，若泄露可能给自然人权利和自由带来高风险，控制者应通知数据主体。

d）完善数据跨境传输机制。GDPR 明确禁止各成员国以增设许可的方式管理跨境数据流动，数据的跨境流动应符合 GDPR 的要求；增加了充分性认定的对象类型；增加了成员国数据监管机构可以指定其他标准合同条款的渠道；将“有约束力的公司规则”（BCR）正式确定为法定有效的数据跨境机制；经认可的行为准则（COC），外加数据控制者/数据处理者落实适当数据保护措施的有效承诺也可以作为数据处理的合法性基础。

e）设立数据保护官。GDPR 规定包括数据控制者和处理者在内的部分组织机构在满足特定要求时应设立数据保护官，数据保护官将监督组织机构内部对 GDPR 的遵守情况，并应担任数据主体和相关监管机构等利益相关方的联络人。

f）巨额罚款，行政罚款分为两档，处以上至 1000 万欧元的行政罚款，或者企业上一财政年度全球年营业额的 2%，按高者计算；处以上至 2000 万欧元的行政罚款，或者企业上一财政年度全球年营业额的 4%，前者罚款主要针对违反控制者或数据处理者的相关义务等，后者罚款主要针对违反处理基本原则、违反数据主体权利和跨境数据传输违法行为等。

2）面对欧盟出台的《一般数据保护条例》，云服务商需要满足其

要求的合规场景主要有以下四种：

a）云服务商在欧盟境内设立分支机构，即欧盟企业从事的数据处理活动，即使实际的数据处理活动不在欧盟境内发生。【控制者或处理者】

b）云服务商的直接注册用户有来源于欧盟，无论该注册用户是否购买云服务。云服务商可能存在对该用户注册信息的处理和分析，云服务商作为数据的控制者存在。【控制者】

c）云服务商的直接用户有来源于欧盟，且该用户已购买云服务，云服务商可能对该用户的资源信息等进行处理和分析，云服务商作为数据控制者存在。【控制者】

d）云服务商的直接用户是非欧盟用户，但该用户面向欧盟提供服务，若其中涉及欧盟数据主体个人信息的处理，云服务商需要遵守 GDPR 要求。【处理者】

3. 新加坡

新加坡借鉴欧美个人信息保护的优点，致力于个人数据保护法在企业层面的可执行性，同时也采取了较多的安全措施，在数据跨境传输、数据保护官等方面都进行了要求。

《个人信息保护法》（PDPA），规定若境外收集的个人数据被传输至新加坡境内，此类个人数据的处理适用于该法案。2013 年，为加强个人信息保护领域工作，新加坡专门设立个人信息保护机构“新加坡

个人信息保护委员会”，对《个人信息保护法》的实施进行日常监督。PDPA 明确了企业的数据管理义务，要求各机构委任一名隐私专员，负责遵守信息保护法律。PDPA 规定了数据跨境转移的条件，跨境数据传输接收方应有不低于 PDPA 保护标准的数据保护水平。

云服务商应满足新加坡《个人数据保护法》要求的的特殊场景如下：

a）云服务商在新加坡境内从事的数据处理活动，即使该企业仅仅作为境外企业的数据媒介，那么虽然数据收集行为发生在境外，云服务商仍需要遵守新加坡《个人数据保护法》的要求。【处理者】

b）云服务商的用户来自新加坡，作为跨境数据传输接收方云服务商应具有不低于新加坡《个人数据保护法》保护标准的数据保护水平。【控制者或处理者】

4. 美国

美国采取以行业自律和市场调节机制为主的松散立法，对数据保护采取“长臂管辖”原则，扩大了执法部门对境外数据的权限，同时对于儿童信息数据、电子通讯数据等特殊数据进行了立法保护。

《澄清境外数据的合法使用法案》于 2018 年 3 月 23 日生效，它进一步扩大美国执法部门访问海外数据的权限，使执法机构要求访问海外数据更为容易，而不管数据存储在哪个国家。

《儿童网上隐私保护法》要求网络从业者要确实告知其用户网站

的隐私权政策；面向 13 岁以下儿童收集信息之前，必须首先获得其家长可验证的事先同意，要求网站保证父母有可能修改和更正这些信息。

《电子通讯隐私法》，该法案是目前保护个人电子通讯信息最全面的一部联邦法案，它涵盖了声音通讯、文本和数字化形象传输等所有形式的数字化通讯，不仅禁止政府部门未经授权的窃听，而且禁止所有个人和企业对通讯内容的窃听，同时还禁止未经授权地拦截或访问传输或存贮于电脑系统中的通讯信息。

美国各州《安全泄露通知法案》，该法案对数据泄露通知进行了要求，例如，有些州规定数据泄露涉及的被害人数超过 500 人时应当通知政府主管部门。

《2018 加州消费者隐私法案》，该法案被称为美国“最严厉、最全面的个人隐私保护法案”，定于 2020 年 1 月 1 日生效，并广泛适用于收集加州消费者个人信息的企业。法案为消费者创建了访问权、删除权、知情权等一系列消费者隐私权利：访问权：消费者有权要求收集个人信息的企业向消费者披露其收集的信息类别和具体内容；删除权：消费者有权要求企业删除其所收集的任何个人信息；知情权：消费者有权知道其个人信息被卖去何处，企业必须发布有关消费者的个人信息如何被出售或披露以及披露给谁（或哪些第三方）的信息。在罚则方面，企业违反隐私保护要求将面临支付给每位消费者最高 750 美元的赔偿金以及最高 7500 美元的民事处罚。

5. 加拿大

加拿大数据保护相关立法主要从数据收集、处理、使用等方面对企业进行要求，同时赋予用户一定的权利。

《隐私保护法》对约 150 个联邦政府部门和机构在收集、使用和披露个人信息时进行限制，以尊重公民隐私权；同时该法案赋予公民获得由联邦政府机构持有的其本人的个人信息，并予以更正的权利。

《个人信息保护和电子文件法》,规范的对象是从事个人信息商业运作的机构，包括与信息采集、使用和披露相关的作业。要求任何个人信息经营机构都能够尊重 CSA 模范规则确定的“公平信息利用原则”,法律体现原则共有 10 个,它们分别是:承担保密义务的原则;确定采集和使用个人信息的目的原则;当事人同意的原则;有限采集原则;限制使用、披露和存储的原则;准确性原则;保证个人信息得以安全保存的原则;公布使用方法原则;当事人有知情权原则;接受申诉并核实信息的原则。

6. 日本

《个人信息保护法》修订版于 2017 年 5 月 30 日正式生效。是日本保护个人信息安全的主要法律，该法案确立了个人信息保护的基本原则及方针。该法案对个人敏感信息进行了特殊保护，明确对个人敏感信息的处理须经本人明示同意;对“匿名加工”情况下的数据删除权进行了要求;对数据跨境传输中涉及到的

外国第三方提出了限制；同时也规定了经营者公开披露的义务。

7. 韩国

《个人信息保护法》于2011年正式实施。该法案的基本原则是指导和规制个人信息保护的立法及执法，指导个人信息保护行为和解决侵犯个人信息争议的基础性规范。为保障“个人信息自决权”，该法案从以下几个方面进行了规定：1. 个人信息的收集者应明确个人信息的处理目标和范围，以必要性为限制收集和处理数据；2. 安全管理个人信息；3. 公开处理个人信息的方针，保障信息主体阅览请求权等权利；4. 匿名处理，降低对信息主体私生活的侵害；5. 指定隐私官。同时，该法规定通过设立专门的个人信息保护委员会、引入个人信息影响评价制度，构建韩国全方位的个人信息保护体系。

表 1 各国数据保护法律法规对比表

	数据保护官	数据主体权利	数据要求	泄露通知	特殊数据保护	跨境传输	特殊要求
中国《网络安全法》		知情权 删除权 纠正权	明示同意 处理合法性 数据安全性	√		√	● 适用于所有的“网络运营商”，包括网络的所有者、管理者以及利用他人所有或者管理的网络提供相关服务的网络服务提供者，包括基础电信运营者、网络信息服务提供者、重要信息系统运营者等。 ● 引入“关键信息基础设施”的概念，并对

							“关键信息基础设施”的运营者提出了严格的跨境传输规范。 ● 要求网络运营者应当按照规定留存相关的网络日志不少于六个月。 ● 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。
欧盟 GDPR	√	访问权 纠正权 删除权 迁移权 知情权 拒绝权	明示同意 数据处理合法性 数据安全性 处理记录保存性 匿名处理	√	未成年人数据	√	● 适用范围包括数据控制者或数据处理者设立在欧盟，或数据主体为欧盟境内主体，且数据处理行为涉及向该主体提供服务或监控其在欧盟的行为。 ● 个人数据泄露时，控制者应在 72 小时内向监管机构报告，若泄露可能给自然人权利和自由带来高风险，控制者应有义务通知数据主体。 ● 明确禁止各成员国以许可的方式管理跨境数据流动，将“有约束力的公司规则”（BCR）

							正式确定为法定有效的数据跨境机制。 ● 违反 GDPR 条例的最高罚款金额为 2000 万欧元或者公司全球营业额的 4%。
新加坡《个人数据保护法》	√	访问权 纠正权 知情权	默认同意+选择性退出 处理合法性 数据安全性			√	● 要求组织在必要的情况下，尽可能准确和完全地对每个访问请求在 30 天内作出响应，如果不能满足这个要求，该组织必须（在 30 天内）以书面形式通知申请人它将对请求作出响应的时间。 ● 规定了数据跨境转移的条件，跨境数据传输接收方应有不低于新加坡保护标准的数据保护水平。
日本《个人信息保护法》		访问权 删除权 纠正权 停止使用权	默认同意+选择性退出 处理合法性 数据安全性 处理记录保存性 匿名处理			√	● “个人信息”的含义包括从个人身体信息转换的代码，如指纹数据、人脸识别数据、声带振动和 DNA 碱基序列。 ● 个人数据匿名化转移到第三方时，企业必须根据规定创建匿名数据，并确保原始的匿名化数据不能被重新创建。 ● 在没有数据主体同意的情况下，企业被禁止获取诸如种族、宗教或医学历史等敏感数据。 ● 企业接收第三方数据时需确认个人数据的获取方式，并在一段时间内保留个人数据被接收的记录。 ● 法律适用于为了在日

							本境内提供服务而收集的个人信息，即使该信息的处理发生在境外。 ● 网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；
韩国《个人信息保护法》	√	访问权 选择权	处理合法性 数据安全性、匿名处理				● 公共组织和私营企业经营者禁止无法律依据的收集、使用和处理居民身份证信息。 ● 如果一个实体没有采取措施确保安全漏洞导致了居民注册号码的泄漏，该实体可能会受到高达五百万韩元的罚款。

各国对数据保护态度不同，立法内容也有差异，但无论严苛或宽松，大致可归纳为如下几项要求：1、个人数据的定义，范围不断扩大；2、设立数据保护专员；3、数据主体的权利，包括知情权、删除权、纠正权等；4、数据保护义务，包括数据完整性、数据安全性等；5、对个人敏感信息进行特殊保护；6、跨境传输要求，何种情况下可以进行跨境传输；7、数据泄露披露，包括报告监管机构，通知数据主体；8、对特殊类型数据的处理，如儿童数据等；9 成立独立的监管机构。

(四) 国内外数据保护相关标准

1. 信息安全技术 个人信息安全规范

《信息安全技术 个人信息安全规范》于 2017 年 12 月 29 日由中

国国家标准化管理委员会正式发布。该规范参考了个人信息保护方面通行的国际准则、国外的最新立法和权威的国际标准等，从国家标准层面明确了企业收集、使用、分享个人信息的合规要求，为企业制定隐私政策及个人信息管理规范指明了方向，其具体要求涉及个人信息保护的全流程，具体可分为六大方面：一是个人信息的收集需满足合法性、最小化、授权同意等要求，同时明确提出收集个人敏感信息时需要明示同意；二是个人信息的保存需满足保存时间最小化、去标识化、加密等要求；三是个人信息的使用需进行访问控制、展示限制、更正删除限制等；四是个人信息的委托处理、共享、转让、公开披露、跨境传输要求等；五是个人信息安全事件的应急处置和告知上报等；六是组织管理需明确职责分工、进行相关人员管理培训、安全审计等。资料性附录部分列出了个人信息示例、个人敏感信息判定、保障个人信息主体选择同意权的方法以及隐私政策模板。

2. ISO/IEC 27018：公有云个人隐私保护认证

ISO/IEC 27018 是国际标准化协会制定的一项国际标准，是公有云个人隐私数据保护方面的首个国际标准。ISO/IEC 27018 要求公有云服务提供商需要满足以下五个关键指标：

1）同意(Consent)：

云服务提供商应保证用户享有充分的个人隐私，不得使用其接收到的个人信息用于广告或营销，除非用户有明

确要求。

2）控制(Control)：

用户享有对其储存数据完整的控制权，服务商必须将对数据的操作告知用户并得到认同。

3）透明度(Transparency)：

云服务提供商必须告知用户，他们的数据是如何被储存以及存储于何处，披露被“分包商”们所使用的二级流程，并且需要对如何处理这些数据做出明确的承诺。

4）沟通(Communication)：

若出现意外，云服务提供商需告知用户、并清楚地保留本次事故的记录和响应方式。

5）独立性和年度审计(Independent and yearly audit)：

云服务提供商的独立第三方审计需保持文档的一致性，其监管义务必须值得用户信赖。此外，云服务提供商还必须接受每年一次的第三方复核。

3. CISPE 个人数据保护行为准则

欧洲云计算服务供应商联盟(CISPE，Cloud Infrastructure Services Providers in Europe)作为欧洲云计算领导者联盟，其准则提供的个人数据保护合规架构可协助云用户评估供应商的云端基础设施服务是否可用来处理个人数据，确保符合行为准则的云服务提供商不会因为自身目的存

取或使用用户资料。

CISPE 个人数据保护行为准则的制定参照欧盟《一般数据保护条例》，该准则可以帮助云服务提供商更好地遵循 GDPR 的要求，符合该行为准则的云服务提供商可以让云用户选择将资料完整的存放在欧盟经济体内并进行处理。

4. 云服务用户数据保护能力参考框架

《云服务用户数据保护能力参考框架》是中国信息通信研究院“可信云服务”系列标准在数据安全领域的深化，该标准从用户视角出发，提出了云计算用户数据保护参考框架，一方面为云计算企业建立规范完备的用户数据保护体系、保障用户数据安全提供指导，另一方面为第三方机构对云计算服务提供者的用户数据安全保护能力评估提供依据，同时也为用户选择数据能够得到良好保护的服务提供参考。

该标准规定了云计算数据保护能力的十六大类指标，全面覆盖数据安全事前防范、事中保护和事后追溯三个阶段，使企业在达到“可信”的基础之上，实现对“安全”的全面保障。事前防范指标包括：数据持久性、数据私密性、数据知情权、数据防窃取性、数据可用性、数据访问安全性、数据传输安全性、数据迁移安全性、数据销毁安全性、数据返还安全性和服务可审查性；事中保护指标包括：入侵防范、恶意代码防范；事后追溯包括应急响应、安全审计、用户投诉与反馈。

二、个人数据保护原则

基于各国在个人信息保护方面的法律要求及国内外数据保护相关标准，在数据主体权利和数据保护义务方面的共通要求，结合经济合作与发展组织（Organisation for Economic Co-operation & Development)提出的个人信息保护八项原则，云服务商个人数据保护应遵守以下原则：

（一） 合法性原则

个人数据的收集和处理应满足法律监管要求、保证处理过程的正当和透明，同时应征得数据主体或儿童监护人的同意。

（二） 目的限制原则

个人数据的收集目的必须特定、清晰、合法，且在收集时确定。数据处理过程中不得违背或超出该目的。

（三） 数据质量原则

数据使用应限于数据处理目的充足、相关和必须的范围之内，且数据必须准确、完整、适时更新。

（四） 公开和知情原则

企业应及时进行必要的信息披露，并确保个人有权了解数据的存储位置、使用程度等信息。

（五） 安全性原则

数据处理方式应当确保个人数据安全，包括采取适当技术和组织措施，防止数据被非法或非授权处理，或意外丢失、破坏和毁损。

（六） 责任原则

企业应保证其本身在个人数据处理中的合规，要求关联公司、第三方服务提供商、承包商及代理满足合规条件，并对上述原则负责。

三、云服务商个人数据保护措施

（一） 数据由云服务商控制

对于个人数据的保护，在不同场景下应明确数据是由云服务用户控制还是由云服务商控制。当个人数据主体为云服务的直接用户时，数据由云服务商控制，如图 3 所示。

这种情况下，面对各国个人数据保护的法律监管要求，云服务商可以采取以下措施提升其自身的个人数据保护能力。

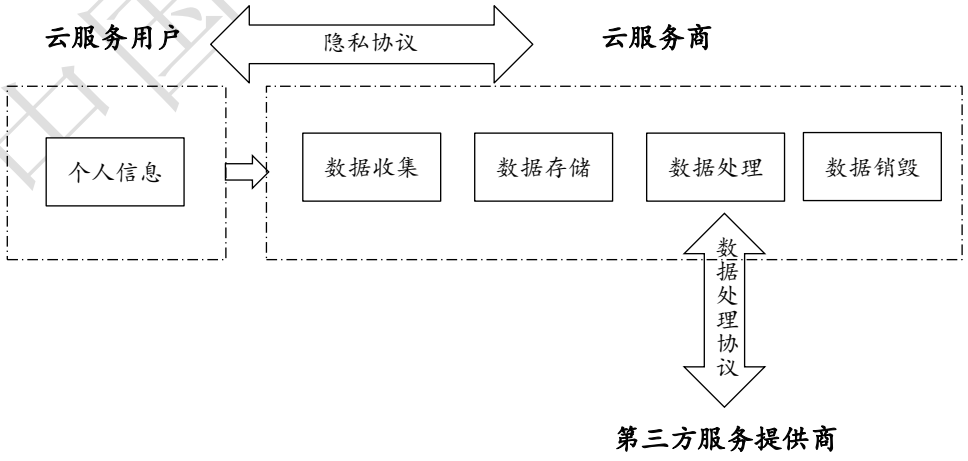


图 3 数据由云服务商控制时的数据处理流程示意图

1. 建立跨部门合作

个人数据保护的合规不只是安全或者法务部门凭一己之力可以完成的任务，至少需要安全、法务、管理部门、开发部门、运维部门、财税部门等相关部门共同组建合规团队，在协作下才能完成个人数据保护的合规工作。企业高层管理人员应高度重视个人数据保护工作，积极牵头成立合规团队，以保证相关工作的有效推动。

2. 标准化的隐私协议

隐私协议是企业对收集、保存、使用等个人信息处理行为的公开法律承诺，是政府、社会监督企业个人数据保护的重要依据。企业应根据相关法律法规，以易于访问的方式公开隐私协议，协议内容应清晰易懂，隐私协议中包括但不限于：

1）数据收集、保存、使用等环节相关信息的说明，应明确告知数据安全措施和保护能力等；

2）个人信息的共享、转让及公开披露声明；

3）个人信息主体的权利，包括知情权、删除权、纠正权等；

4）隐私协议生效时间；

5）协议变更相关条款与用户通知方式；

6）数据泄露通知，包括通知时限、通知方式等；

7）企业联系方式。

协议涉及的具体指标项，可参考国内相关标准，并结合需满足的法律法规予以补充调整。

3. 个人数据保护措施

1）隐私保护理念贯穿产品设计

企业在构建产品或服务时，应全面融入数据保护理念，让安全从早期介入，才能避免后期因产生安全事故导致更严重的企业损失。PbD（Privacy by Design）理念被誉为保护隐私的最佳实践案例，企业可参考 PbD 七大原则，将隐私理念植入产品或服务的技术架构。

2）升级数据安全管理制度

企业应注重内部的隐私管控，从人员聘用要求到数据安全管理规章，应不断修订更新，以匹配数据保护方面法律法规的要求。对不同类型的相关人员应区分操作权限，设置内部审批流程，并做相应记录。

3）建议企业设置专职的数据保护人员

企业应设立专职的数据保护人员，与跨部门的合规团队合作，建立起从决策层到执行层的安全管理组织架构和人员管理机制。

4）提高工作人员数据保护意识

企业应针对技术负责人及相关员工进行专门的隐私保护培训，建立隐私保护流程，避免人员误操作带来的数据泄露事故。

5）提高数据全生命周期的安全保护能力

a）明确获得用户的授权同意或符合其他例外情形

企业应以明显且清楚的方式告知用户将会采集哪些数据以及这些数据的主要用途，特别是涉及到未成年人时，必须获得监护人的直接授权同意。

b）个人数据的保存和敏感信息的存储传输

企业对个人信息的保存期限应严格受使用目的所需时间限制，在超出期限后应进行删除或匿名处理；对于个人敏感信息的传输与存储，应进行加密或其他技术处理。如：记录身份证号时，隐藏中间的生日数据段，避免因数据泄露而直接能够定位或指向某一个可识别的自然人。

c）个人信息的使用限制

企业对个人信息的使用不得超出收集时个人信息主体授权同意的范围；对个人信息进行展示时企业应采取去标识化处理。

d）数据的跨境传输

在需要进行个人信息跨境传输时，企业应严格遵循我国及相关国家的法律要求。

e）保障个人信息主体权利

企业应依据相关法律法规，保障个人信息主体对其个人数据的访问、更正、删除、撤回及获取副本等权利，涉及第三方处理者的，企业应及时与第三方处理者同步信息。个人信息主体提出申诉的，应及时做出响应回复。

f）安全事件的处置、告知和报告

企业应制定个人信息安全事件应急处理预案，承诺在数据泄露时立即采取补救措施，按照法律法规的要求及时告知个人信息主体并向有关部门报告。

4. 规范第三方合作

当数据由云服务提供商控制，云服务商在委托第三方处理个人信息时，不得超出个人信息主体授权同意的范围，并依据相关法律法规要求第三方实施适当的技术和组织机制，通过合同规定、签订数据处理协议或审计等方式对第三方进行约束和监督。在第三方无法履行其数据保护义务的情况下，应声明云服务商仍然对云用户完全负责，承担其委托处理者的义务。

5. 第三方评估

云服务商可定期参加第三方关于个人信息或隐私保护的认证评估，如 ISO/IEC 27018、CISPE 个人数据保护行为准则认证、云计算风险管理能力评估、云服务用户数据保护能力评估等，通过第三方视角挖掘企业在个人数据保护领域的盲点，定期开展个人数据保护能力风险评估，梳理协议规范性和技术薄弱点，规范企业行为，提高企业个人信息保护能力。

（二） 数据由云用户控制

当数据由云用户控制时，云服务商仅负责处理数据（如：电商

企业将自己的网站部署于云上，用户在网站上的登陆信息、购买信息等数据存在云上），如图 4 所示。

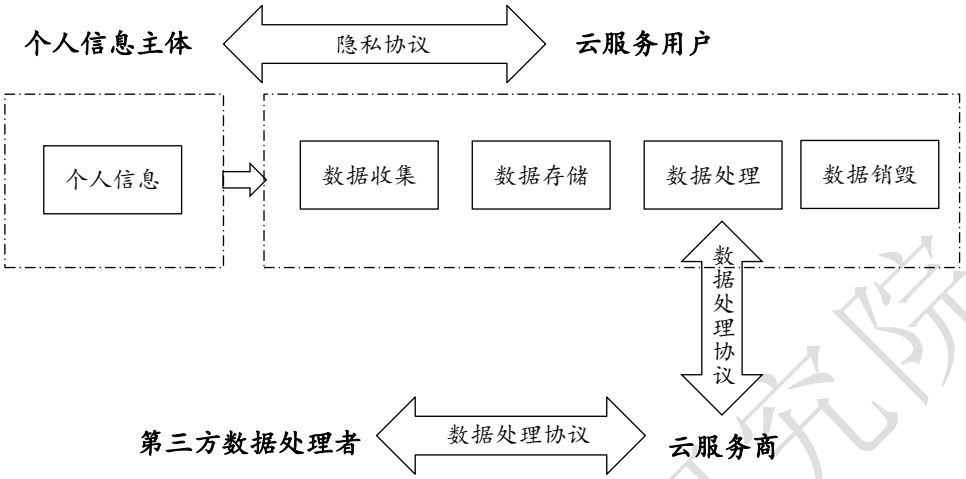


图 4 数据由云服务用户控制时的数据处理流程示意图

企业可采取以下措施规范自身行为，并提供相关数据安全服务帮助云用户满足各国关于个人数据保护的法律监管要求。

1. 标准化的数据处理协议

云服务商仅负责处理数据时，建议与云用户签订数据处理协议，规范云上数据的存储和管理，保障云用户的数据安全。协议内容包括但不限于：

1）云服务提供商信息披露；

2）数据处理保密性和安全性；

3）子处理者的授权与责任声明；

4）用户权利；

5）数据泄露事件的通知；

6）监控或审计；

7）赔偿与保险；

8）协议变更相关条款与用户通知方式。

协议涉及的具体指标项，可参考国内相关标准，并结合需满足的数据保护法律予以补充调整。

2. 数据处理安全措施

1）升级数据安全管理制度

企业应注重内部的隐私管控，从人员聘用要求到数据安全管理规章，应不断修订更新，以匹配相应数据保护法律法规的要求。

2）规定企业、第三方及相关人员的保密义务

云服务商应明确承诺除必要的维护或提供服务的目的之外，企业不会访问、处理或使用用户数据。同时，云服务商应通过合同或权限设定等措施限制相关企业人员、第三方处理者或其他分包商处理未经授权的用户数据。

3）建议企业设置专职的数据保护人员

企业应设立专职的数据保护人员，与跨部门的合规团队相合作，建立起从决策层到执行层的安全管理组织架构和人员管理机制。

4）保证数据的物理安全

企业应明确如何保证数据所在设备的物理安全，防止未经许可的设施访问，包括设置物理屏障、安装视频监控、制

定人员身份审核政策等。

5）保证数据的网络安全

企业应明确如何保证数据的网络安全，阻止未经许可的网络访问，包括防火墙的使用和身份验证控件等。

6）数据安全传输方案

企业在设计系统架构时，需具备数据安全传输的解决方案，在传输过程中确保数据的加密性、完整性，并进行严格的双向身份认证。

7）数据安全事件的处置和通知

企业应制定数据安全事件处置的应急预案，承诺在发生数据泄露、丢失等安全事件时立即采取补救措施，并按照法律法规的要求及时告知相关云用户。

8）定期测试、评估

企业应对其服务的安全性进行定期审查，根据行业标准衡量其信息安全规范性和措施的合理性，并及时对服务进行维护和更新。

3. 规范第三方合作

对于云服务商来说，企业在数据保护问题中涉及与云用户、其他分包商等角色的协同合作。企业应格外注意与外部的合作，确保其他合作者具有相应的数据保护能力，通过签订数据处理协议明确权责划分，避免合作中因一方行为不当导致的连带责任。

1）与云用户签订数据处理协议

当数据由云用户控制，云服务商仅负责处理数据时，云服务商应依照相关行业标准与云用户签订数据处理协议，规范云上数据的存储和管理，保障云用户的数据安全。

2）数据处理供应链的安全管理

当云服务商在数据处理中引入第三方处理者或其他分包商，或数据处理过程涉及第三方产品或服务时，云服务商应确保第三方处理者或分包商的数据保护能力，对数据处理的产品和服务的供应链进行严格的安全管理，并通过数据处理协议明确双方责任义务，避免由于第三方服务商出现数据泄露问题而产生的连带责任，将数据安全事故的风险降到最低。

4. 为用户提供数据安全服务

云用户负责数据的控制时，应满足各项适用的数据保护法，对数据安全负有责任。云服务商可以为云用户提供数据安全服务或产品，如匿名、加密、备份、定期测试等，帮助云用户更好地履行其对数据主体的义务，为云用户在数据生命周期内的合规提供保障。云服务商与云用户在数据保护中责任共担，云用户数据保护水平的提高，也将降低云服务商数据保护的难度。

5. 第三方评估

企业可定期参与第三方关于数据处理安全及数据处理协议的认证评估，如：中国信息通信研究院云服务用户数据保护能力评估、

云计算风险管理能力评估等。行业第三方权威认证为云服务商保障用户数据安全提供指导，定期开展个人数据保护能力风险评估，帮助其建立规范完备的数据保护体系，有效规避相关风险。

6. 云服务保险保障

面对数据保护相关的风险问题，云服务商可以通过购买云计算服务责任保险（简称“云保险”）建立一套事前风险评估，事后保险赔偿的模式，构建云计算风险管理的完整链条。发生数据丢失或数据泄露等问题时，企业可以接受第三方客观的定损定则，界定事故责任和事故损失，保险公司根据定损报告实际赔付相关损失，从而将风险转移给保险公司，有效降低云上数据风险，保障云上数据安全。

四、总结

个人数据的泄露或被窃取，轻则导致公民财产损失，重则引发刑事案件，给人们的生命财产安全带来严重风险隐患。个人数据的保护问题涉及每个公民的切身利益，在全球范围内受到高度关注。各国纷纷出台个人数据保护方面的法律法规，旨在遏制个人数据非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益。

云服务商应根据相关法律法规制定标准化的隐私政策，成立专门的安全团队负责数据保护相关工作，加强数据从收集、使用、传输到销毁全流程的安全技术能力建设，提高云服务的数据保护能力，保护个人数据安全。同时，云服务商可以为用户提供匿名、加密、

备份等数据安全产品或服务，帮助用户更好地履行其对数据主体的义务，为用户在数据生命周期内的合规提供保障。

附录

一、 腾讯云

1. 个人数据保护概览

对于个人数据保护,腾讯云一直承诺,“数据是客户的重要资产，未经客户授权，绝不主动触碰客户数据”。因此，腾讯云关注并持续遵从各国对个人数据保护的合规要求，包括史上最严的 GDPR 合规要求。今年 5 月，腾讯云国内首家通过了 GDPR 合规框架下的 CISPE 认证。

CISPE 是欧洲目前唯一提供符合 GDPR 合规要求的行为准则的非营利性组织，通过合规准则提出了更强大的数据保护、治理和合规要求，客户信息的安全无疑将受益。CISPE 的认可是腾讯云的云服务符合 GDPR 合规要求的又一个强有力的证明。

在此之前，为了保证客户的云环境安全可靠，腾讯云已通过二十（20）种国际认可的合规标准认证。 腾讯云平台拥有中国内部最全面的认证，如 ISO/IEC 27018 公有云个人信息信息保护国际认证，CSA STAR 云安全认证，信息安全管理 ISO 27001 认证，PCI DSS（支付卡行业数据安全标准）认证，业务连续性管理 ISO 22301 认证，IT 服务管理 ISO 20000 认证，质量管理 ISO 9001 认证，由中国工信部数据中心联盟评估的可信云服务认证。我们致力于构建一个更好的云环境，并通过获取最新且定期更新的认证和合规标准来保证。

用户注册腾讯云时，需要阅读并同意腾讯云提供的关于个人数据处理过程的协议，数据隐私和安全附录（DPSA），符合 GDPR 标准的 DPSA 也是为用户实现 GDPR 合规性做好准备的一种工具。

2. 安全产品/服务

腾讯云在全球众多地区和可用区域建立和维护基础设施，安全可靠、性能卓越，通过在腾讯云上构建兼容 GDPR 标准的基础架构，提供大量专业的云技术服务，帮助客户的业务实现 GDPR 合规。

腾讯云数盾数据安全服务拥有多个云安全服务产品解决数据管理、保护、日志和审计的需求，以促进客户在整个数据生命周期内符合 GDPR。

数据管理模块让客户对敏感数据的分发一目了然，对客户数据库执行漏洞扫描和威胁警报，并对批量数据传输进行脱敏。

数据保护模块提供访问控制、加密和智能脱敏。它们与日志和审计模块一起，在数据处理原则、设计与默认数据保护、处理安全和活动记录、向监管当局通报数据泄露，以及数据传输保护方面满足 GDPR 的要求。

数据审计模块具备强大的 AI 威胁检测引擎，即使面对非常严峻的安全环境，依然能够轻松预测变化，将各类新出现的变体攻击通报给管理员，帮助企业从容应对各种形态的攻击。

3. 腾讯云 GDPR 合规服务

为了帮助客户和合作伙伴评估、分析、整改并最终满足 GDPR 的要求,腾讯云联合全球领先的信息安全咨询服务公司提供额外的GDPR合规咨询服务。通过整合云计算与云安全产品和服务，使得腾讯云与合作伙伴和客户共同遵守 GDPR 中数据保护、数据治理和合规性的要求，其中包括敏感数据分布视图、访问控制、加密、脱敏、审计、安全测试及告警等。

如我们的客户所期待，腾讯云对数据保护、数据治理和合规性有着坚定的信念。除了一如既往地向客户提供安全可靠的符合 GDPR 合规性的云环境之外，我们还将继续在我们的云环境中开发安全解决方案,不断扩展我们的产品/服务,从而使客户不仅能满足 GDPR 的要求，还能满足不断更新的隐私监管要求。

二、 京东云

用户隐私和个人信息的保护，不仅是社会各界高度关注的问题，也是京东最为重视的工作之一。自创立以来，京东秉承“诚信为本”“正道成功”的价值观，坚持对假冒伪劣商品“零容忍”，因此赢得了广大用户的信赖，获得了业务持续发展的动力。京东始终坚信，保护用户隐私和个人信息，不仅是企业的法定责任，更是京东不断发展的内在需求。因此，在个人信息保护和隐私政策的建构方面，京东云坚持以“用户信赖”为立足点，为用户隐私和个人信息保护的实现，构建起相对完善的数据管理体系和实现数据安全的技术与产品保障。

1. 高标准的数据安全治理体系

为了加强对于用户个人信息的保护和数据安全，京东云从安全治理、安全管理、安全运营建设三个维度开展数据安全，特别是个人信息保护的合规管理工作。京东云也因此获得了国际先进的 ISO27001 信息安全管理体系认证。

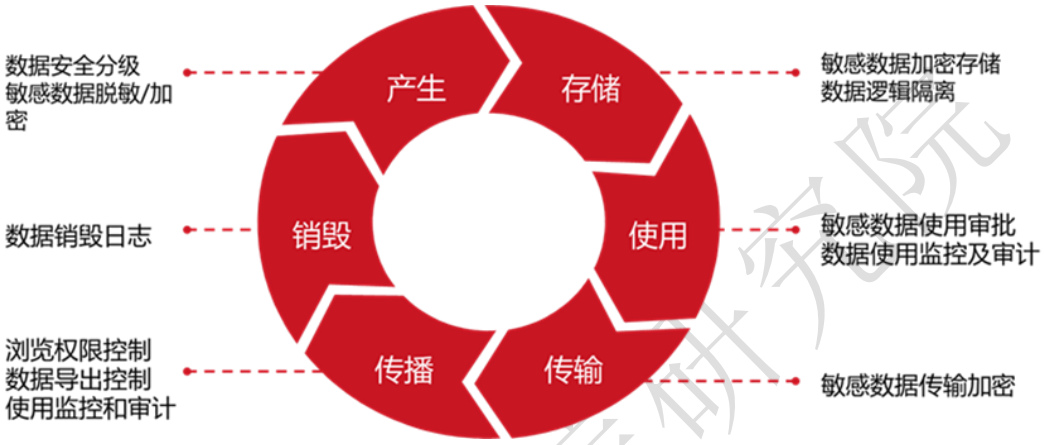
一是安全治理。成立专门的安全治理团队，从收集、传输、存储用户数据的载体，即云产品、系统出发来保护用户数据。保证云产品、系统的安全是保护用户数据的基本要素。京东云从产品、系统开发之初应进行安全咨询沟通，对产品安全分析，严格掌控安全开发流程，并不断的进行问题追踪处理。保障了产品和系统在设计之初、开发之中、使用之后都对其安全性进行实时跟踪，确保为用户数据提供保障。

二是安全管理。包括安全管理机构的建立，设立的专门的安全岗位，负责数据安全相关政策、方向、重大安全项目的决策和指导。设置安全执行工作人员，负责相关的安全响应、梳理、治理等行动执行。通过安全组织加强整体安全方面的管理和方向的把握。

三是安全运营。设置专门的运营团队。运营团队不仅负责解决外部对云平台的攻击的问题，同时负责对内部人员的违法、违规操作进行审计，及时发现内网的风险，保护用户数据。建立应急响应机制，负责一旦云平台发生数据泄露等事件，能够在第一时间响应，并将损失降低到最低，保护用户数据。设置安全复盘计划，不断发现和优化现有的安全机制、流程和技术，做到未雨绸缪，保护用户数据。

2. 加强数据生命周期各环节的安全技术能力建设

除了高标准的数据安全治理体系，京东云还通过加强数据生命周期各环节的安全技术能力建设，不断提高用户的个人信息保护水平。京东云获得了中国信息通信研究院颁发的“可信云”认证。



一数据分离。云平台使用逻辑隔离将每个用户的数据互相分离开来。分离提供多用户服务的缩放和经济优势，同时严格防止用户访问其他人的数据。

二静态数据保护。用户负责确保按标准加密云平台中存储的数据。云平台提供各种加密功能，便于用户选择满足自己需求的最佳解决方案。帮助用户保持对密钥的控制，以便云应用程序和服务用于加密数据，使用云磁盘加密来加密虚拟机，存储服务加密可以加密用户存储帐户中的所有数据。提供各种数据存储解决方案，以满足不同需求，包括文件、磁盘和表存储等。

三密钥管理。借助密钥管理服务（Key Management Service，KMS），用户可以安全、便捷的使用密钥，专注于业务需要的加解密功能场景及应用。

四传输中数据保护。云产品控制台上的通信都受到了 HTTPS 安全协议的加密保护。使用行业标准传输层安全性的 SSL/TLS 加密在用户与云，云平台系统和数据中心之间的内部通信，保护传入或传出组件的数据，以及在内部传输的数据。

五数据冗余。出现网络攻击或者数据中心遭到物理损坏时，可确保数据受到保护。用户可以选择：出于合规或延迟方面的考虑使用国内存储或出于安全或灾难恢复目的使用国外存储。数据可在选定的地理区域中进行复制以实现冗余，但不会传输到此区域以外。用户可以使用多个选项来复制数据，包括指定副本数量，以及复制数据中心的数量和位置。

六数据销毁。当用户删除数据或离开京东云时，京东云会在重复使用之前遵循严格的规则覆盖存储资源，并对已退役的硬件执行物理销毁。在用户提出请求和合同终止时，京东云会执行完全数据删除。当某个存储设备已达到其使用寿命的最后时期时，京东云程序中包括的退役流程可防止用户数据暴露给未授权的个人。将根据行业标准实践对所有退役的磁性存储设备进行消磁和物理销毁。

三、 华为云

1. 个人数据保护概览

华为是全球领先的 ICT 基础设施和智能终端提供商。经过三十多年的高速发展，华为的业务已覆盖全球 170 多个国家和地区，拥有 18 万、160 多种国籍的员工，海外本地化率 70%，在 2018 年世界 500 强

排名榜单中已跃居第 72 位。

在合规经营方面，华为依托自身丰富的全球化运营经验，从政策、流程、组织与文化等方面建立了完善的管理体系，确保公司遵守所有开展业务国家的法律法规，为海外业务的顺利开展保驾护航。华为理解社会对个人数据保护的关切，对个人数据保护高度重视，已将个人数据保护纳入华为商业行为守则中，并于 2016 年发布了个人数据保护总体政策，系统性地阐述了华为在个人数据保护方面的政策，用于指导华为遵守所有开展业务国家适用的个人数据保护的法律法规，并定期持续向员工提供数据保护的培训以增强员工的意识。

华为云作为华为公司的战略发展重点，秉承华为对个人数据保护的总体政策，并以更高的标准严格执行，在业界率先提出了**“公有云三不原则”**，即上不做应用，下不碰数据，不做股权投资。其中，“不碰数据”意味着华为云不用技术手段获取客户的数据，不会强迫客户跟华为云进行数据的交换。**在商业模式的选择上，要“靠技术和服务变现，不靠用户数据变现”。**同时，华为云开放人工智能和大数据的平台为客户处理数据，让客户的数据发挥价值，塑造智能社会。

华为云沿用华为公司在个人数据保护上的成熟实践，将要求融入日常业务活动中，且在整个业务生命周期内，研发、运营、运维、安全专家及法务人员紧密协作，从各环节充分落实执行个人数据保护各项要求。

除坚持遵循各类个人数据保护的法律法规外，华为云还依托内部审计部门完成了全面的技术和流程审视，并已通过多项业界公认的国

际、国内标准的认证和鉴定，包括：

1）国际标准的 ISO 27001、CSA-STAR、PCI-DSS 第 1 级认证；

2）国内工信部数据中心联盟评估的可信云服务认证、公安部安全等保 4 级认证；

3）2018 年华为云更是**全类服务、全平台、全节点通过专注云中个人数据保护的 ISO27018 认证**。

2. 华为云数据安全产品/服务

华为云对租户提供一系列云服务，协助客户快速满足个人数据保护合规要求，包括但不限于：

数据加密服务：

数据加密服务是一个综合的云上数据加密服务。它提供专属加密、密钥管理、密钥对管理等功能。

当客户使用对象存储、云硬盘、镜像服务和关系型数据库等服务时可使用密钥管理功能（密钥管理功能已在上述服务中集成，客户不用单独调用数据加密服务）。该功能可对密钥进行全生命周期集中安全管理，且客户主密钥由保存在拥有主流国际安全认证的硬件存储模块（HSM）中的根密钥进行加密。

当客户有更高的合规性需求或需要在云上延续传统物理密码机的使用经验时，可以使用专属加密功能。该服务将通过国家密码局认证或 FIPS 140-2 第 3 级验证的硬件加密机或其虚拟化实例提供给客户，满足客户更高的安全性需求。

数据加密服务详细介绍：

https://www.huaweicloud.com/product/dew.html

数据库安全服务：

华为云数据库安全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。该服务内置了多种行业合规知识库（HIPAA、SOX、PCI DSS 等），客户可以自行定义敏感数据、动态脱敏等策略。其中脱敏引擎依据策略对使用中的数据进行实时动态脱敏，既不影响应用性能及原始存储，又避免了敏感信息泄漏。

数据库安全服务详细介绍：

https://www.huaweicloud.com/product/dbss.html

云审计服务：

云审计服务提供的日志审计功能以及与之配套的安全能力，可助力客户轻松通过常见信息系统安全设计、标准体系建设的合规性审核。

其优势包括：1）审计日志格式统一，所含内容符合常见标准的规定 2）审计日志的产生、传输、存储过程均采用高强度加密，传送过程安全可靠；3）一键开通，无需维护，支持将操作记录合并，低成本的长久保存。

云审计服务详细介绍：

https://www.huaweicloud.com/product/cts.html

安全合规专家服务：

为了帮助客户评估、分析合规需求，华为云还提供了安全合规专

家服务。目前已上线《网络安全法》安全合规专家服务。

《网络安全法》安全合规专家服务详细介绍：

https://www.huaweicloud.com/solution/cel.html

关注我们

中国信息通信研究院

地　　址：北京市海淀区花园北路52号
邮政编码：100191
联系电话：010-62304839
传　　真：010-62304980