

隐私保护设计（PbD）研究报告

——PbD 照亮数字未来，合规要求变为信任礼物



全球法律政策研究院

既是实干家，也是学术派

2021

序言

作为隐私和数据保护的核心理念，PbD（Privacy by Design）是企业合规工作的重要一环，它将保护要求以技术手段运用到产品和服务的形态设计中，成为通往合规“源头管控”的一条必由之路，也是学术界、产业界的探索热点和关注重点。

合规的“数据”蕴藏巨大的“资源”价值，PbD的导入可最大程度确保数据的原生“合规”性，因而受到监管方、相关方和企业的多重重视，积极投入资源开展实践探索。PbD作为一项隐私和数据保护的有力手段，整体发展仍处于起步阶段，但在实践上已呈现出显著“始发特点”下的强烈“分化趋势”：在广度和深度上仍存在诸多空白，但强者在技术和理念上已遥遥领先。

企业产品创新的加速和个人隐私保护的觉醒对冲下，PbD正成为取得二者平衡的“粘合剂”。法律法规持续完善的外部压力，在数字创新产品竞争的内部动力，使得PbD日益广泛地展示在我们身边，启示着科技本质的初衷：服务用户，满足客户，尊重客户，保护客户。

可以预见，PbD将不再是企业产品设计成本、合规加固成本的可选项，而是基础项。它将决定着企业能否建立客户信任，使产品更具有生命力，更决定着企业和产品能否拿到数字时代的市场竞争入场券——如题所述，PbD照亮数字未来，合规要求变为信任礼物。

申楠

目 录

1. PbD 基础认知.....	2
1.1. PbD 由来.....	2
1.2. PbD 内涵与基本原则.....	2
1.3. PbD 实施理念和步骤.....	3
1.4. PbD 应用现状与发展趋势.....	4
2. PbD 工作指南.....	5
2.1. 通用指南.....	5
2.2. 行业指南.....	6
2.2.1. 车联网.....	6
2.2.2. 虚拟语音助手.....	7
2.2.3. 视频设备.....	8
3. PbD 实施策略.....	9
3.1. 数据收集和使用.....	9
3.2. 数据存储.....	9
3.3. 数据对外提供.....	10
3.4. 数据删除/销毁.....	10
4. PbD 合规要求.....	10
4.1. 权利保障.....	10
4.2. 安全责任.....	11
4.3. 特殊处理.....	12
附录： PbD 实践范例.....	14
A. 数据生命周期维度.....	14
B. 监管热点对象维度.....	18
参考文献.....	21

隐私保护设计 (PbD) 研究报告

1. PbD 基础认知

1.1. PbD 由来

隐私保护设计 (Privacy by Design, PbD) 源自进入信息时代后公众对于隐私的担忧。经济数字化加速了数据的广泛使用, 在收集、存储、传输、使用、共享、删除等数据生命周期的各个阶段, 隐私和数据合规风险贯穿始终。以数据收集为例, 看起来收集只要符合个人知情和同意的要求, 但实践中保护个人免受“过度”或“未经授权”的数据收集是一项艰巨的挑战, 黑客、网络钓鱼者等会采取各种方法, 开发新的手段和技术来不当获取数据。

个人和企业均希望能够对隐私数据进行充分保护, 控制风险并对抗挑战。**就个人而言**, 能力和心理上的局限性使得他们无意或无法恰当有效地保护隐私和个人数据。**就企业而言**, 法律规定和政策指南往往只提供基本要求, 没有明确具体的技术组织措施和统一的评判标准, 只能根据法律法规要求去研究、制定符合自己业务的隐私保护框架, 探索、开发隐私保护的实现方法。

隐私保护设计 (Privacy by Design, PbD) 是解决个人和企业隐私保护关切的优选路径之一。**价值导向设计理论** (Value Sensitive Design)、**代码之法** (code as law, law as code)、**隐私增强技术** (Privacy Enhancement Technology), 均在尝试利用技术的力量来保护隐私, 尝试将公平信息实践原则直接嵌入到信息通讯技术的设计和运行当中, 利用技术和代码的力量来保护隐私。随着产品服务的快速迭代和隐私保护的日益复杂, 依靠技术来保护隐私的理念得以进一步拓展, **隐私保护设计这种综合技术、运行系统、工作流程、管理结构、物理空间和基础设施的保护理念应运而生。**

1.2. PbD 内涵与基本原则

PbD 将隐私保护的用户导向原则引入到软件、服务设计和使用的各个环节中, 将隐私保护前置, **主张在系统设计的最初阶段将隐私和数据保护的需求“嵌入其中”, 成为系统运行的默认规则, 而不是事后简单地“附加其上”。**

2009 年 8 月, 安·卡沃基博士发布《隐私保护设计: 七项基本原则》一文, 提出了隐私保护设计应当遵循的七原则¹:

¹ **积极预防, 而非被动救济。**隐私保护设计理论主张采取积极预防的态度, 而非被动救济的立场, 不要等到个人信息风险已经明朗化或侵害发生后, 再去提供事后的救济, 而应从一开始就考虑如何预防和阻止侵害的发生。

隐私默认保护。隐私保护设计理论主张, 隐私和数据保护应当成为企业商业实践和系统运行的默认规则。如果用户不做任何放弃个人信息的选择, 那么他们的个人信息应当是完好无损的。例如, 许多浏览器将 Cookies 设置成默认关闭状态, 以便让用户的浏览数据不被追踪。

将隐私嵌入设计之中。隐私保护设计理论主张, 隐私和数据保护的需求应当嵌入到系统的设计之中, 成为系统的核心组成部分, 同时又不损害系统的功能。例如, 电脑主机上的 BIOS 密码设计、手机的防盗功能设计、笔记本电脑的指纹识别设计等, 都贯彻了这一原则。

功能完整——正而非零和。隐私保护设计理论反对将隐私和数据保护与功能、效率、安全、商业利益等价值对立的零和方式 (zero-sum, win/lose), 主张通过正和方式

- (1) **积极预防，而非被动救济。**
- (2) **隐私默认保护。**
- (3) **将隐私嵌入设计之中。**
- (4) **功能完整——正和而非零和。**
- (5) **全生命周期的保护。**
- (6) **可见性和透明性。**
- (7) **尊重用户隐私——确保以用户为中心。**

1.3. PbD 实施理念和步骤

PbD 的实施因适用范围不同而有所区分。产品设计角度，立足软件开发和用户界面设计。例如，软件开发过程中，根据数据交互和分享等环节的风险，应用适当的隐私保护技术进行风险防控。用户界面设计上，让隐私相关的说明、采集信息的告知更加醒目、易懂，确保用户理解隐私条款的内容，帮助用户了解隐私工程技术能够保护相应敏感信息。实施策略设计角度，兼顾“开发设计”和“运营设计”。例如，最小化、隔离、隐藏、聚合等面向数据的策略更侧重于对数据本身的处理，其技术性更强；通知、控制、执行、证明等面向过程的策略更侧重于处理个人数据的业务过程。实施策略可以融合应用在产品全生命周期中，用于产品开发设计阶段可以用较低的成本有效提高产品隐私保护的能力，用于在运营设计阶段可以有效消减产品和服务的数据合规风险。

在基本原则和实施理念的指导之下，业内概括提出了 PbD 的实施步骤：

- (1) **界定法律需求；**
- (2) **系统功能分析；**
- (3) **确定数据范围和类型；**
- (4) **隐私风险分析；**
- (5) **多边需求分析；**
- (6) **方案的实施和测试。**

七大原则为制定更为详细的隐私和数据保护标准提供了总体参考框架，而六大步骤作为落地实施参考，每一步骤的采用和具体实施都需要经过事先的周密讨论和实践探索。例如，在**界定法律需求**方面，企业需要根据所在地、经营地等法律法规要求来制定需要遵从的合规框架。一般而言，全球化运营的企业往往选

(positive-sum, win/win) 来实现隐私和数据保护，实现用户、企业等多方共赢。

全生命周期的保护。隐私保护设计理论主张隐私和数据保护的需求在用户数据被首次收集之前就嵌入系统设计之中，并扩展至系统运行的整个生命周期，提供从摇篮到坟墓全过程的保护。

可见性和透明性。隐私保护设计理论主张企业商业实践和系统都应当依据公开的承诺和目标来运作，并接受独立核查，即隐私保护设计的具体内容和实施必须具备可见性和透明性。

尊重用户隐私——确保以用户为中心。隐私保护设计理论主张，最好的隐私保护设计都是围绕用户的需求和利益展开的，让用户在管理个人信息中扮演积极角色，或许是防范隐私风险最为有效的措施。例如，在微信朋友圈设置中，腾讯就给予了用户很多选择，体现了对用户隐私的尊重，包括可以看谁的朋友圈、不看谁的朋友圈、允许陌生人查看十张照片、允许朋友查看朋友圈的范围等。

择以《通用数据保护条例》(GDPR) 作为合规框架的遵从标准, 在其结合业务所在国的法律要求进行加持, 其法律需求体现为: (1) **数据处理的合法性基础**; (2) **数据主体的权利范围及保障**; (3) **第三方数据交互的合法共享和接收**; (4) **数据存储和销毁的合法依据**; (5) **数据保护的技术和组织措施要求 (包括数据安全事件的应急处置要求)**。相应的, PbD 以及产品的功能分析、安全措施等落地也以此作为基础依据和基准参考。

1.4. PbD 应用现状与发展趋势

近年来, 为贴合科技发展中对隐私和个人数据的保护需求, PbD 理论和实践得到了发展, 相关研究的深入和文件的发布正不断完善着 PbD 体系建设。其中需重点提及的是欧盟 GDPR², 其中第 25 条明确提出数据控制者须遵守“**设计及默认的数据保护**”(data protection by design and by default, 以下简称为“DpbDD”)义务, 并应采取适当的措施和必要的保障, 通过**设计和默认设置方式**以有效地实施数据保护原则继而保护数据主体的权利和自由。而基于对 DpbDD 的重视, 欧盟数据保护委员会 (EDPB) 于 2020 年 10 月通过了《关于 GDPR 第 25 条设计及默认的数据保护指南》, 其以要求结合案例的形式, 将 PbD 理论与 GDPR 的实践进行了充分指导。

此外, 英国 ICO《数据保护指南》³, 西班牙 AEPD《默认数据保护指南》, 印度《2019 个人数据保护法案 (送审稿)》, 新加坡 PDPC《ICT 系统的数据保护设计指南》等国家和地区法律法规, 以及国际数据保护和隐私委员会《隐私设计方案》(Resolution on Privacy by Design), 美国 FTC《隐私设计新框架》⁴以及国际标准《ISO/IEC 27701, 安全技术-扩展的 ISO/IEC 27001 和 ISO/IEC 27002-隐私信息管理要求和指南》等, 都充分吸收、借鉴和发展了 PbD 理论。

回望中国, 中国虽未发布文件以从字面上规定 PbD, 但《民法典》《网络安全法》《数据安全法》《个人信息保护法》等法律法规, 已然从数据处理者义务角度将 PbD 理念落地。例如, 《个人信息保护法》第五十一条进一步规定: 个人信息处理者应当根据个人信息处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等, 采取下列措施确保个人信息处理活动符合法律、行政法规的规定, 并防止未经授权的访问以及个人信息泄露、篡改、丢失: **(1) 制定内部管理制度和操作规程; (2)**

² GDPR 第 25 条——数据系统保护和默认保护 data protection by design and by default

1. 考虑到国家的发展水平、实施成本和处理行为的性质、范围、环境和目的, 以及处理可能给自然人的权利和自由带来的风险和损害, 控制者在决定和实施数据处理的方法时, 应当以一种有效的方法实施适当的技术、组织措施, 例如设计来实施数据保护原则的匿名机制和数据最小化机制, 并且将必要的保障措施融入到处理之中以使数据处理既符合本条例的要求又保护数据主体的权利。

这一条款要求数据控制者通过设计保护个人数据在数据收集前便设置好保障个人隐私不受侵犯的措施

2. 数据控制者应当实施相应的技术和组织措施以确保在默认 (by default) 情形下, 被处理的个人数据对每个特定处理目的都是必要的。此项义务适用于一定量的个人数据的收集, 一定规模上的处理, 这些数据的存储和它们的可访问性。尤其是这些机制应当确保在默认的情形下, 个人数据在缺乏个人介入时是不能被不特定数量的自然人所访问的。”

这一条款要求数据控制者通过默认方式设置数据保护措施。

³ 英国 ICO《数据保护指南》(the Guide to data protection), ICO (Information Commissioner's Office) 是英国维护信息权的独立机构, 具有执法权, 采取一定的行动来确保企业履行其信息权利和承担义务。其近期关于 PbD 的最新实践如下: ICO 裁定英国皇家医院与 Google 的 Deep Mind 数据共享协议违反了数据保护法。在《数据保护指南》中专门设立了“隐私保护设计 (PbD)”的章节, 对其进行了说明, 鼓励企业将隐私保护设计纳入现有的项目管理和风险管理方法和政策中。

⁴ 2012 年美国联邦贸易委员会提出了隐私设计新框架, 主要提出了三个核心原则: 通过设计保护隐私, 简化选择和透明度。在隐私保护设计新框架中, FTC 对 Facebook、Google 等互联网公司不符合 PbD 理念的做法进行了举例, 实施了制裁。例如 Facebook 曾在数据使用和共享的文字说明方面, 向用户使用了误导性的语句, Facebook 告诉消费者, 第三方应用程序只能访问应用程序需要运行的用户信息。事实上, 应用程序可以看到几乎所有用户的个人数据。FTC 因此对 Facebook 实施了制裁。

对个人信息实行分类管理；（3）采取相应的加密、去标识化等安全技术措施；（4）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；（5）制定并组织实施个人信息安全事件应急预案；（6）法律、行政法规规定的其他措施。

法律条文虽未在词汇上未描述为 PbD，但实际上包含了 PbD 的内容和精髓，要求个人信息处理者在个人信息处理活动中应采取必要措施。例如，通过对个人信息实行分级分类管理、采取相应的加密、去标识化等安全技术措施确保个人信息处理活动的合法性和个人信息的安全。

法律条文之外，一些标准规范也在一定意义上直接回应 PbD 要求，并不同程度地体现了 PbD 精神。以 ISO/IEC 27701:2019《安全技术 ISO / IEC 27001 和 ISO / IEC 27002 的扩展：隐私信息管理—要求和准则》为代表，诸多的国际标准试图从系统设计、建立、实施、维护和持续改进入手，为企业如何处理隐私和数据保护并保障自身安全义务提供详尽指南。相关标准还包括：ISO/IEC 27550:2019《信息技术 安全技术 系统生命周期过程的隐私工程》、ISO/IEC 29151:2017《信息技术 安全技术 个人可识别信息保护的实践准则》、ISO/IEC 27018:2019《信息技术 安全技术 公共云作为个人识别信息 (PII) 处理者的个人识别信息保护实践导则》等，我国的《信息安全技术 个人信息安全规范》、《信息安全技术 个人信息安全工程指南（征求意见稿）》等也是 PbD 理念的落地指导。

2. PbD 工作指南

2.1. 通用指南

2014 年，欧盟网络和信息安全局（ENISA）报告中正式提出了八项隐私保护设计策略：（1）最小化，（2）隐藏，（3）隔离，（4）聚合，（5）通知，（6）控制，（7）强制/执行，（8）证明。2019 年，中国全国信息安全标准化技术委员会首次在工作组会议上发布了《个人信息安全工程指南》，前述八种设计策略被《个人信息安全工程指南》（2019-4-第一版）沿用并明确列举至附录 C.1 中。示例如下：

设计策略	说明	隐私控制示例
最小化	处理个人信息的量尽可能限制在最小数量	在你收集之前选择； 匿名化/假名
隐藏	个人资料，他们的人际关系，从全貌中隐藏	数据的存储和中转加密 混合网络 隐藏流量模式 基于属性证书 匿名化/假名
隔离	个人信息尽可能在分布式方式，分离的部分中处理	点对点排列 隔离和虚拟化

聚合	个人信息以最高水平聚集在一起并确保尽可能少的细节仍然有用。	聚合超时（在智能计量使用） 动态位置粒度（基于位置的服务中使用） k-匿名 差分隐私
通知	透明度	隐私首选项平台 数据泄露通知
控制	数据主体提供给机构对他们的个人信息的处理	用户为中心的身份管理 端至端的加密支持控制
强制/执行	与法律要求相适应隐私政策予以强制执行	访问控制 粘性政策和隐私权管理
证明	证明符合隐私政策和所有适用的法律要求	隐私管理系统 日志记录和审计的使用

英国 ICO (Information Commissioner's Office) 对于“设计及默认的数据保护”实施情况专门提供了检查清单，作为“通用标准”的一种倡导建议。示例如下：

☐ 我们将数据保护问题作为设计和实施系统、服务、产品和业务实践的一部分。
☐ 我们将数据保护作为处理系统和服务的核心功能的重要组成部分。
☐ 我们在风险和侵犯隐私事件发生之前就进行预测，并采取措施防止伤害个人。
☐ 我们只处理实现我们目的所需的个人数据，并且只将数据用于该目的。
☐ 我们确保在任何 IT 系统、服务、产品、和/或业务活动中，都会自动保护个人数据，不需要个人采取任何具体行动来保护他们的隐私。
☐ 我们提供组织内部及个人的数据保护负责人的身份及联络信息。
☐ 我们在公开文件中采用“简单明了”的政策，使个人很容易理解我们对其个人数据的处理。
☐ 我们为个人提供工具，使个人可以决定我们如何使用他们的个人数据，以及我们的政策是否得到适当地执行。
☐ 我们提供强大的隐私默认值、用户友好的选项和控制，并尊重用户的喜好。
☐ 我们只使用能充分保证其技术及组织措施符合设计的数据保护的数据处理者
☐ 当我们在处理活动中使用其他系统、服务或产品时，我们确保只使用那些设计者和制造商考虑到数据保护问题的系统、服务或产品。
☐ 我们使用隐私增强技术（PETs）来帮助我们遵守设计的数据保护义务。

2.2. 行业指南

通用指南外，行业领域基于对行业数据特征，制定针对性的要求。例如，EDPB 第 01/2020 号《在联网车辆和出行相关应用环境下处理个人数据的指南》、EDPB 第 3/2019 号《关于通过视频设备处理个人数据的指南》、EDPS《隐私设计保护的初步意见》均不同程度涉及了对各自领域内隐私保护设计的具体要求。

2.2.1. 车联网

EDPB 第 01/2020 号《在联网车辆和出行相关应用环境下处理个人数据的指南》的规定充分体现隐私保护设计兼顾“开发设计”和“运营设计”的要义。示例如下：

通用实践介绍	解决方案示例
汽车和设备制造商、服务提供商和其他数据控制者应当，如可行，使用不涉及个人数据或不涉及传输个人数据到车外的流程（例如，数据在内部进行处理）。	在车内处理数据的环保驾驶应用，在车载屏幕上实时显示环保驾驶建议； 涉及在用户的完全控制下（例如通过蓝牙或 Wi-Fi）传输个人数据到一台设备（例如智能手机）上的应用，并且车辆的数据不会传输给应用提供商或汽车制造商；这包括，比如，连接智能手机以使用汽车的显示、多媒体系统、麦克风（或其他传感器）打电话等，只要收集的数据保持在数据主体的控制之下，并且仅用来提供数据主体要求的服务； 车载安全增强应用，例如在驾驶员超车却没有打信号或驶出白线时提供方向盘声音信号或振动，或就车辆状况提出预警（例如，就影响刹车片的磨损提出预警）；
敏感数据诸如生物识别数据、关于犯罪行为或其他违法行为的数据以及详细的位置数据的处理需要处于用户的完全和唯一控制之下（本地化处理），否则这些数据的处理需遵守更为严格的规则。	使用驾驶员的生物识别数据解锁、启动和/或激活某些车辆指令的应用，这些生物识别数据存储在车内（例如面部或声音模型或指纹特征）。
汽车制造商、服务提供商等作为数据控制者或数据处理者时，必须开发安全的车载应用，并且遵守设计和默认隐私的原则。	EDPB 推荐开发一个安全的车载应用平台，与安全相关的汽车功能进行物理分离，以便对汽车数据的访问不依赖于不必要的外部云能力。 汽车制造商和服务提供商应尽可能考虑本地数据处理，以减轻云处理的潜在风险。
用户应当能够控制他们的数据在车辆中被收集和处理的方	关于处理的信息必须以驾驶员所使用的语言提供（包括手册，设置等）； EDPB 建议，只有对于车辆运行所必需的数据才能被默认处理。对于任一其他目的和控制者/处理者，数据主体都应可以考虑数据处理的目的和合法基础，激活或停用该数据处理，并且可以删除有关数据； 数据不能传输给任何第三方（即，用户拥有对数据的唯一访问权）； 数据的保存时间不得超过提供服务所需的时间，或欧盟或成员国法律规定的时间； 数据主体应能在出售车辆前永久删除所有个人数据； 数据主体可以在可行的情况下直接访问这些应用程序生成的数据。
虽然不是每一用例都可诉诸于本地数据处理，但通常可以采取“混合处理”的方式。	在基于驾驶行为的保险中，关于驾驶行为的个人数据（例如，施加在制动踏板上的力度、行驶的里程数等）既可以在车辆内部处理，也可以由车载信息系统服务提供商（telematics service provider）代表保险公司（数据控制者）进行处理，并生成分数，将这些分数按一个确定的周期（例如按月）传输给保险公司。这样一来，保险公司无法访问原始的行为数据，而只能访问作为处理结果的总分。这可以确保数据最小化的原则从设计着手得到满足。这也意味着，当数据由其他方存储时，用户应当具有行使其权利的能力，例如，在 GDPR 第 17 条的条件下，用户应具有删除存储在汽车维修店或经销商系统中的数据的能力。

2.2.2. 虚拟语音助手

2021 年 3 月，欧盟数据保护委员会 (EDPB) 发布了 EDPB 第 02/2021 号《虚拟语音助手指南 (征求意见稿)》⁵，为虚拟语音助手的提供者、开发者等遵守“设计及默认的数据保护”义务提供具体的指引。

- 虚拟语音助手的提供者和开发者应考虑其每项功能**是否必须要有一个注册用户**。
- 管理日程或通讯录显然需要一个注册用户，但打电话或上网搜索功能要求虚拟语音助手拥有注册用户是否必要目前并不是那么清晰。
- 默认情况下，不需要识别用户的服务**不应该通过命令关联任何识别用户**。隐私和数据保护友好的默认虚拟语音助手只会为了执行用户请求处理用户数据，**而不会存储语音数据或已执行命令的记录**。
- 有些设备只能运行一个虚拟语音助手，而其他设备可以在不同的虚拟语音助手中选择。虚拟语音助手提供者应根据 GDPR 第 20 条的规定制定行业标准，以**实现数据可携带**。
- 一些虚拟语音助手提供者声称，即使数据主体提出要求，他们的虚拟语音助手也不能删除所有的用户数据。虚拟语音助手提供者应确保根据 GDPR 第 17 条的规定，**应用户的要求删除所有的用户数据**。

2.2.3. 视频设备

2019 年 7 月，欧盟数据保护委员会 (“EDPB”) 发布了《关于通过视频设备处理个人数据的指南 (征求意见稿)》并于 2020 年 1 月正式通过该指南⁶，为视频监控行为中的数据控制者遵守“设计及默认的数据保护”义务做出指引。

- 控制者需要在**计划进行视频监控时就实施适当的数据保护技术和组织措施，即在开始收集和处理视频录像之前**。
- 控制者首先应评估对基本权利和自由的影响，并考虑采用较少侵入性的手段来实现其合法的处理目的。这些原则强调需要内置增强隐私的技术、最小化处理数据的默认设置，以及提供必要的工具，使个人数据得到最大程度的保护。
- 控制者不仅应将数据保护和隐私保障措施纳入技术的设计规范中，而且应将其纳入组织实践中。**组织实践方面，控制者应采用适当的管理框架，建立和执行与视频监控有关的政策和程序**。技术角度来看，系统规格和设计应包括根据 GDPR 第 5 条所述原则处理个人数据的要求（处理的合法性、目的限制、GDPR 第 25 (2) 条规定的默认情况下的数据最小化、完整性和保密性原则、以及问责制等）。如果控制者计划购买商用视频监控系统，需要将这些要求包含在购买规范中。
- 控制者需要确保在系统的整个生命周期内，将这些要求应用于系统的所有组件和由其处理的所有数据。

⁵ https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-022021-virtual-voice-assistants_en

⁶ https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

3. PbD 实施策略

3.1. 数据收集和使用

PbD 重点在于数据收集和使用的最小化、通知和控制策略的落实。在数据收集和使用环节，产品/服务的研发设计和运营强调数据最小化的收集使用，数据主体应得到充分的告知及提供必要的工具以使个人数据得到充分的保护。若在个人数据处理过程中产生新的个人数据时，亦应遵从个人数据保护的相关监管规定。

- 某科技企业 PbD “最小化”策略表现突出，其整体隐私政策和预装 App 隐私政策相互配合，将个人信息收集的范围与业务功能一一对应。此外，某智能家居厂商将设备数据作为个人信息予以保护和设计，主动扩大个人数据范围的界定以提高数据合规化获取的方式。
- 在云服务领域，云服务提供商大部分严格区分了用户的“账户数据”和“业务数据”，以严格划分自身的数据保护范围。
- 目前大部分企业采用在用户本地设备端实施利用生物识别信息进行的身份识别、认证，企业在服务器端仅接收验证结果而不收集用户生物识别信息。这种处理策略是“最小化”结合技术实操落地良好体现，即从技术角度出发避免了收集至服务器端的必要性。
- PbD “控制”策略除体现在儿童及其监护人的控制外，某 ICT 企业通过面部识别功能及提供的“防后台录音、拍照”功能（当应用在后台调用麦克风、摄像头等权限时会进行提醒或默认拦截）实现的隐私控制表现可谓优秀。
- PbD “通知”策略中，某云服务商除隐私政策外，还采用了 FAQ 的形式向客户阐明了与其隐私和数据保护相关的各种问题，这种简明易懂的方式值得借鉴。

3.2. 数据存储

在存储环节中，PbD 实施重点在于数据存储的最小化、聚合、隐藏策略。即除相关法律法规另有规定或数据主体另有授权外，个人数据的存储期限应为实现数据主体授权使用目的所必需的最短时间，超出该等存储期限后应对个人数据进行删除和匿名化处理。对于数据的存储应采取分类分级措施，对于敏感个人数据采用更为严格的保护措施。

此外，我国《个人信息安全规范》鼓励个人信息控制者在收集个人信息后，宜立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。EDPB 的《设计及默认的数据保护指南》还强调应实施默认设置，以防止任何未经授权的数据访问和存储。

可信执行环境——TEE(Trusted Execution Environment)、本地存储分析、虚拟化处理并隔离存储用户信息等这都是这方面的优秀实践案例。

3.3. 数据对外提供

中国法律法规对于数据共享环节的监管要求远远高于境外。因此，建议企业考虑遵从较高的法律法规的要求，即详细披露数据接收方的身份和联系方式，对外提供的信息类型，提供目的及接收方数据安全能力，提供方式若包含 SDK 的，还需要遵守额外的 SDK 安全管理和披露规范。同时应注意，中国的数据对外提供的监管目光主要集中于第一手数据处理者，该数据处理者对于数据接收方如何使用数据等具有高度关注义务。因此，若作为第一手数据处理者，在数据对外提供的 PbD 实践中应考虑对接收方设计相应的监督策略。

3.4. 数据删除/销毁

数据销毁，即在数据保存不再具备处理数据的合法目的或用户撤回同意或产品/服务终止运营等情形下，相关数据应及时删除数据并承诺不会进行数据恢复。达到特定密级的数据，应根据风险评估结果确定是否采用必要的安全销毁方式。

除了 NIST 800-88《数据清理指南》⁷外，DOD（美国国防部）与 NIST（美国国家标准与技术研究院）针对数据销毁问题还发布过诸多指南，为实现使媒体上的目标数据在一定程度上无法访问，这些指导文件中提供了诸如 7 次以上覆写、加密擦除、消磁、物理销毁等不同等级的清除方式。

实践中，可借鉴的数据销毁方法包括：**将随机数据多次写入相关存储硬盘扇区中；在备份前对数据进行加密，通过将该等加密密钥与特定的保存期限关联起来，只要销毁特定密钥，就可销毁相关所有数据。**

4. PbD 合规要求

4.1. 权利保障

数据主体权利保障是法律法规在 PbD 中重要的关注内容。例如，GDPR 中强调的 DPbDD 的核心义务在于采取适当的措施和必要的保障，通过设计和默认设置方式以有效地实施数据保护原则继而保护数据主体的权利和自由；印度《2019 个人数据保护法案（送审稿）》中也强调在个人数据处理环节的每个阶段都应考虑数据主体的利益。

当前，除若干科技企业外，大部分数据控制者仅提供指定页面或客服沟通的渠道，用户自主更正、删

⁷ <https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final>

除其个人信息的交互设计显著欠缺。

中国监管非常重视数据控制者对“账户注销权”的保障，并鼓励采用交互式页面（如网站、移动互联网应用程序、客户端软件等）提供产品或服务的数据控制者，应直接设置便捷的交互式页面提供功能或选项，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利。

4.2. 安全责任

PbD 设计中，安全责任属于与传统数据安全重合较多的一部分。为有效保障数据的完整性、机密性和可用性，数据控制者应采取技术措施和其他必要措施防止数据泄露、篡改、丢失及损毁，《个人信息保护法》中对于个人信息处理者的安全责任作出了相对全面的要求，包括但不限于：

- (1) 建立健全内部数据安全管理制度和操作规程；
- (2) 对数据实施分级分类管理；
- (3) 采取必要的加密、去标识化等安全技术措施；
- (4) 合理确定个人数据处理的操作权限，并定期对相关人员进行安全教育和培训；
- (5) 指定个人数据保护负责人并公开负责人姓名和联系方式；
- (6) 定期审计个人数据处理活动；
- (7) 加强风险监测，对个人数据处理活动进行安全影响评估；
- (8) 建立健全数据安全事件的应急处理、报告和通知制度。

企业可通过如下步骤建立隐私保护框架：

(1) **设计合适的隐私控制环境，提供企业实施内部控制基础。**在此过程中，应遵从指导性原则：a.体现对诚信和道德价值的承诺；b.行使监督责任；c.建立结构、权利和责任；d.体现对能力的承诺；e.加强问责制。同时，可以通过确保董事会的参与、建立授权和职责，以及配置适当的团队来满足前述原则。

(2) **建立隐私风险评估机制，明确合适的目标、识别并分析风险、评估欺诈风险、识别并分析重大变更等。**在风险评估过程中，企业应充分考虑：

- 法律法规因素：包括违规成本，新兴关注领域、立法和执法活动等；
- 合同因素：包括行动者之间达成的协议，公司策略及相关公司规则等；
- 业务因素：包括设想的应用及其使用情境的特征，行业指南、行为准则、最佳实践或标准；
- 其他因素：隐私偏好与个人信息主体，内部控制系统、技术标准，声誉成本、内部文化成本等。

综合上述各方面因素，建立风险评估、风险处置的流程，明确相关的沟通、评审等要求。

(3) **基于风险评估结果，选择并制定适用的控制活动，建立执行隐私控制的责任人和问责制。**

(4) **有效沟通隐私保护要求。**通过制定相关政策和开展培训以在内部有效沟通控制目标 and 责任声明；通过制定透明的隐私政策等，保证与外部各方（包括监管机构）的沟通清晰一致等。

(5) **建立覆盖不同评估范围和评估频率的评估机制。**持续性监控机制和针对具体问题的独立评估机制。企业可根据相关法律法规及监管部门的要求得出评估结果，评估差距应上报至管理层，及时改进产品的隐私保护措施。

4.3. 特殊处理

儿童数据处理。各国对于儿童年龄的界定并不相同，从严遵从相关法律法规的要求非常必要。在处理不满十四周岁的儿童个人数据时，应当征得其父母或监护人的同意，保障未成年人及其父母或者其他监护人的合法权益。根据中国《儿童个人信息网络保护规定》的要求，对儿童隐私和数据保护的监管愈加严格，企业在中国境内处理儿童个人信息时：

- (1) **需建立未成年用户的发现机制，通过注册时的主动填报或服务过程中的验证机制对未成年用户进行认定。**
- (2) **应完善监护人同意机制，如通过短信等方式获取未成年人监护人的明确同意。**
- (3) **企业需注意儿童身份变更后账号的控制权转移，保障用户成年后对账户和个人信息的控制权回收。**
- (4) **企业还应设置专门的儿童隐私和数据保护规则和用户协议、指定儿童隐私和数据保护专员，并通过隔离存储、加密保护等安全保护措施，严格遵守儿童数据合规要求。**

大部分企业均声明未征得儿童父母或其监护人的同意，不会收集儿童个人数据。多数企业将防范收集儿童个人数据的责任归置于家长和监护人身上，且部分企业并未针对儿童个人数据的收集使用设定更为严格的保护措施。但同时也存在一些优秀案例，如某手机厂商只允许监护人为儿童建立专门的儿童账户，并通过“家长模式”和“支付验证”等功能涉及实现监护人对儿童个人信息、购买行为的管理，在儿童数据保护方面充分体现“控制”的策略实践。

老年人数据处理。对于老年人的隐私和数据保护一般遵从成人相关的隐私和数据保护合规要求即可。中国提出了对于老年人隐私和数据保护的额外要求，即在明确互联网网站及移动应用（APP）适老化通用设计规范及评测体系并通过标识授予和企业信用加分等方式来鼓励企业进行适老化改造工作的同时，提出“移动应用程序进行个人信息处理时应遵循最小必要原则，即处理个人信息应当有明确、合理的目的，并应当限于实现处理目的的最小范围，不得进行与处理目的无关的个人信息处理，以保障老年用户个人信息安全。具体收集信息（如位置信息、图片信息等）行为，应符合《常见类型移动互联网应用程序必要个人信息范围规定》《APP 收集使用个人信息最小必要评估规范》要求”。

2021年9月，中国国家发展改革委办公厅发布了《关于推介运用智能技术服务老年人示范案例的通知》，公布了14个地方案例作为第一批运用智能技术服务老年人示范案例。示例如下：

序号	省（区、市）	示范案例	简要内容
1	北京市	北京“健康宝”AI应用赋能老年人便利化出行试点	老年人在“北京健康宝”上注册后，即可使用养老助残卡、身份证等进出各类公共场所，1秒钟左右可以检查完健康状态。
2	上海市	“数字伙伴计划”助力上海老年人跨越“数字鸿沟”，共建人民城市	由政府部门联合企业、市民、社会组织共同发起了解决“数字鸿沟”问题的“上海方案”——“数字伙伴计划”。
3	江苏省	“小江家护”为高龄空巢独居老人安全保驾护航	创建“小江家护”居家上门服务品牌，采取“基础服务+个人定制服务”相结合的方式，为居家老年人提供专业上门服务。
4	天津市	科技赋能 智慧适老——天津市打造银发智能服务平台和智慧康养社区	打造AI银发智能服务平台，提供智能化的居家养老健康服务，为老年人提供跨越医学、营养、运动、心理、社交等多学科融合的健康养老方案。
5	广东省	广东省实现两大全国首创 助力老年人跨越“数字鸿沟”	一证通行，刷身份证进行出入登记和核验健康码的服务功能。
6	山西省	“398贴心保”实时智联 “六助”服务送进家门——“大同助老”蹚出智慧居家养老新路	建设智慧居家和社区养老服务中心，推动助救、助购、助餐、助医、助洁、助行进老年人家门，为老年人搭建线上、线下无缝对接的服务圈。

附录： PbD 实践范例

A. 数据生命周期维度

A.1. 数据收集和使用

A.1.1. 合法性

某科技企业在整体隐私政策中列明包括提供服务、处理交易、进行沟通、保障安全等个人数据使用目的，并言明仅在有合法的法律依据的情况下才会使用用户的个人数据。与此同时，为用户提供了投诉举报的网址，设置了专门的数据保护官负责响应用户关于合法性的疑问。

A.1.2. 最小必要

在某手机厂商官网公开宣传其将数据和隐私保护嵌入产品设计的安全隐私理念，并在隐私政策（更新时间：2019 年 7 月 24 日）文本中表示，将要求用户提供相关个人信息的场景区分为核心业务功能与增值业务功能，**在增值业务功能中，如用户选择不同意收集相关个人信息，增值业务功能将无法实现，但不会影响用户使用核心业务功能。**

在隐私政策中“您的隐私安全”部分，该厂商表明将仅允许产品采集满足业务功能所需的最少量信息，并且信息的采集需要获得用户的明确同意。产品在上线前也会经过隐私合规测试，确保产品实施方案与设计一致。

在“我们保护隐私的措施”部分，该厂商进一步介绍了其在产品设计及开发中采取的隐私保护措施，例如安全键盘的设计：**用户在输入密码等敏感信息时将自动开启，安全键盘不会记录此类敏感信息，不联网、不联想**，从而满足数据收集的最小必要要求。

而当开启该厂商提供的“**保护个人信息**”功能后，应用如需读取联系人、信息等权限，即使已经获得用户的授权，系统仍提供空内容，而无法获得前述信息的全部真实内容。

此外，在该厂商“智能信息服务”中显示，在为用户提供复制验证码、快递查询、一键充值等便捷服务的过程中，用户的短信信息将不会被上传，从而将收集信息范围控制在最小必要范围内。

A.1.3. 知情同意

在设备权限的调用方面，某智能家居 APP 隐私政策以贴近用户的表达方式，采取清晰明了的**表格形式**，分别向用户阐明了 IOS 系统以及 Android 系统调用的系统权限类型，以及调用权限对应的业务功能、调用权限的目的以及调用权限前向用户询问的情况。同时，该企业向用户表明，**如有必要用户可以通过 APP、设备本身（适用于部分设备）或恢复出厂设置来单独关闭部分或全部权限，取消每个联网设备与互联网之**

间的连接等多种方式，拒绝该企业收集相应的个人信息。

某应用程序平台其开发者页面披露，自 2020 年 12 月 8 日起，所有开发者需在其 app 的产品页面上，**使用户能了解到该 app 及第三方合作方（如有）可能收集的数据类型、用途、该数据是否会关联到他们或对其进行追踪、app 隐私和数据保护做法的相关信息**，并以数据控制者主动申报的形式（多维度申报）减轻该厂商作为应用商店运营者的审核责任，该举措将对个人信息主体的告知同意提前到了用户下载 APP 之前，严格强调 APP 开发者及 APP 应用商店的信息披露义务，与中国 APP 合规监管趋势不谋而合。

A.1.4. 单独同意

《个人信息保护法》要求在处理特殊的个人信息或处理个人信息的特殊行为、场景时，个人信息处理者必须就其处理目的、行为等单独向个人告知并取得同意。这种同意模式有四个要件：充分知情、自愿、明确、单独。目前许多企业已经对此进行了特别的功能设计，如某互联网平台的电子证件页面，当服务需要用户填报车辆信息时，该平台会单独说明每个信息字段的处理理由，并让用户在知情和自愿的基础上进行单独的信息填写和提交动作。

“单独同意”的优秀实践案例还有互联网金融企业，其提供的金融服务中需要通过刷脸进行实名认证，涉及处理个人敏感信息应获得用户“单独同意”的合规要求。该企业没有提前索权，**仅在实际业务场景发生时弹出“单独同意”的页面选项**。页面内容仅围绕面部信息授权环节，其中不仅明确说明了处理该敏感信息的目的，还提供单独的《认证服务协议》、《用户授权协议》等文件供用户参阅，并设置为由用户手动点击同意。

上述实践在征得用户“单独同意”方面表现突出，其功能设计较好符合了四要件：**（1）自愿，用户可自由选择开启/关闭。关闭 A 功能不影响 B 功能实现。（2）充分知情：以弹窗形式明确告知用户可行使的权利及途径。用户可通过“了解详细信息”具体了解各项功能及条款说明。（3）单独：每个开关对应单项功能，单项功能下附有必要信息说明。（4）明确：由用户主动点击同意方式，表示同意启用特定功能，并对应收集、处理所需的个人信息。**

A.1.5. 自主选择

某手机厂商针对用户的照片图库细化了访问限制，如果开发者请求访问用户的照片，**用户可以选择仅分享特定的一个或几个项目，或允许访问用户的整个图库**。通过这样的精准控制设置，用户可以不再因为需要上传一张照片而授权 APP 获取整个相册的访问权限，最大程度地实现了 APP 收集信息的最小化与精准性。此外，在位置信息获取方面，该系统允许用户自主选择是否让 app 看到自己的精确位置，从而可以根据服务功能和自身需要灵活控制位置信息的精确程度，这使得用户可以选择在不提供敏感信息的前提下使用需要位置信息才能获取的功能，例如找到附近餐厅或了解当地天气。

某款社交软件**允许用户自主选择个人信息的访问范围**，可以设置的信息包括：好友验证、好友添加渠道、社交空间开关、信息公开范围、好友权限范围、地理位置权限范围等等。用户能够**基于自己的意愿控**

制个人信息的公开范围，并能够随时同意使用、关闭或退出特定业务功能而不影响其他业务功能服务质量。

A.1.6. 安全保障

某手机厂商提供“**防后台录音、拍照**”功能，如，当有应用在后台调用麦克风时，状态栏左侧出现麦克风图标，点击可快速终止录音行为；当有应用在后台尝试调用摄像头时，系统直接拦截，并弹框告知用户风险。此举将避免用户隐私和数据在不知情的状态下被收集。

A.2. 数据存储

A.2.1. 存储时间最小化

某短视频服务平台隐私政策（最近更新时间：2021 年 11 月 1 日）中表明该平台**仅会在为用户提供产品或服务所必需的期间内保留个人信息**，并给出了示例如：当用户使用手机号码注册登录后，平台需要持续保留手机号码，以便提供正常的服务、应对查询和客诉并保障帐号和系统安全；用户未撤回、删除或未注销帐号之前，平台会保留用户发布的内容及相关信息，用以提供持续的业务功能等等。

此外，该平台还针对法律法规有关信息留存的要求给出示例进行说明：“**如果你注销帐号、主动删除个人信息或信息超出必要的保存期限后，我们将对你的个人信息进行删除或匿名化处理**，但以下情况除外：(1) 遵从法律法规有关信息留存的要求（例如：《电子商务法》规定：商品和服务信息、交易信息保存时间自交易完成之日起不少于三年）；(2) 出于财务、审计、争议解决等目的需要合理延长期限的。”

总体而言，该平台从“最小化”理念出发，针对业务必需、法律法规要求等维度通过举例对数据存储期限进行说明，不同类型数据的存储期限仅限于相对应的功能场景，而当存储理由不必要不充分时平台，即会进行删除或匿名化处理，充分落实了“最小化”策略。

A.2.2. 知情权保障

某手机厂商全球隐私政策数据保留时限部分表示，将采取合理的步骤来确保拥有的个人数据准确无误，并删除不正确或不必要的个人数据。保留期限将取决于数据类型以及所涉及的服务或产品。同时，其还使用表格的形式较为直观地向用户展示了各项业务功能涉及的个人数据所需保留的时限。**基于不同业务功能区分数据类型，进而分别确定不同的数据保留时限**并采取表格形式向用户阐明。

A.2.3. 去标识化

根据某手机厂商的最新隐私介绍页面：在地图功能中，从用户的设备发送到地图 APP 服务的数据与随机标识符相关联，这些标识符会在用户使用 APP 的过程中自行重置。地图 APP 利用端到端加密技术在用户的所有设备上保持个人数据同步。**重要地点和收藏均进行了端到端加密**，该厂商无法读取相关内容，因此也不会获知用户的行踪和搜索情况。用户还可以选择采用“模糊处理”方式进行搜索，此时地图 APP 会

进一步在服务器上隐藏用户的位置，在 24 小时后将用户发起搜索的精确地点转化为一个大致的区域，而该厂商不会保留搜索内容或到访地点的历史记录。上述措施旨在实现对用户位置信息的收集使用等方面进行加密处理，且保障了用户对自身位置信息的控制权利，若用户选择通过“模糊处理”方式进行搜索，系统对位置信息的加密措施会更加严格。

此外，浏览器还可安全地监测用户已保存的密码，自动留意可能涉及数据泄露事件的密码。为此，该浏览器运用强大的加密技术，定期对照已遭破解的密码列表来检查用户的密码派生数据。这一过程以安全私密的方式进行，即使该系统开发商本身也不会得知。而一旦浏览器获知泄漏情况的发生，就会帮助用户在可用时升级为“通过其他方式登录”，或自动生成新的安全密码。

A.2.4. 隔离存储

某手机厂商官网明确了数据存储的本地化部署规划，且明确不同区域数据存储将会进行物理隔离，不同的开发者之间的个人数据也会隔离存储。同时，该厂商还在安卓开放环境以外，构建了隔离的可信执行环境——TEE(Trusted Execution Environment)OS，通过分离策略，保护用户敏感数据和业务。具体而言，个人敏感数据不出 TEE OS，生物特征、密钥等敏感数据只存储在 TEE 中，指纹/人脸认证、密码验证等操作全部在 TEE 中完成。有效提高了对敏感个人信息的安全保护力度。

A.3. 数据共享

A.3.1. 告知同意

某手机厂商在隐私政策“我们如何披露您的个人信息”中向用户说明了向第三方披露个人信息的几种情形，表示共享范围将限于本隐私政策声明的、确有必要的个人信息，且其仅会在用户明确同意或法律要求的情况下向第三方披露。而对于其关联方，如果该厂商或关联公司改变个人信息的使用及处理目的，将再次征求用户的授权同意。

需要看到，该手机厂商的做法几乎已经是业内的通行处理方式。随着《个人信息保护法》及相关配套文件、规范和标准的出台，相信告知同意将会取得更加通行和统一的范式。

A.3.2. 最小必要

某手机厂商改进了个人信息共享的保护方面，当手机系统在向 APP 共享用户的位置信息时，将根据信息共享的目的决定是否仅共享用户的大致位置而不是精确位置来加强用户信息保护，例如本地新闻或天气等不需要用户精确位置数据的 APP，而该厂商将仅与之共享用户的大致位置。

A.3.3. 安全保障功能

某手机厂商在隐私政策的第五部分“我们如何保护您的个人信息”中，介绍了其采取的众多安全保障措施，包括加密、访问控制、存储个人生物识别信息前采用技术措施处理、安全培训、相关安全与隐私认证以及将隐私和数据保护要求落实到与第三方的商务合同或审计、考核活动中。

某科技企业在使用第三方供应商的服务器来存储用户的信息时，特别说明会**对这些信息都进行加密处理，并且不会向供应商授予密钥**，因此供应商无法接触用户的数据。该企业将加密密钥保存在自有的数据中心。

A.4. 数据销毁

A.4.1. 最小化

某 ICT 企业支持客户对账户进行注销，且在保留期届满后，客户内容数据会得到彻底清除。并且**提供了云数据迁移服务，有利于用户对拟销毁的数据做好备份**。为用户预留保留期的行为使得该企业在合理期间内仍然保留用户注销的账户信息，在技术上实现了数据注销的最小化需求。

A.4.2. 权利行使渠道

某科技企业通过隐私政策中的链接形式提供了用户删除（注销）账户的途径，明确指出**用户可以出于任何原因随时请求永久性删除账户，通过安全验证后便可删除，即不对用户行使账户注销权施加限制**。同时，该政策还列明了因删除账户而造成不利于用户权益的各项情形，并提供数据查阅与备份的选项，在对用户注销权的保障上符合合规要求。

A.4.3. 删除

某云存储厂商**在客户确认删除操作后，会首先删除客户与数据之间的索引关系，并将内存、块存储等空间进行重新分配前清零操作**，确保相关的数据和信息不可还原，是一种可选的数据清除方式。

B. 监管热点对象维度

B.1. 信息主体权利保障

某科技企业在隐私政策中声明了个人信息主体获知、访问、更正、传输、限制处理和删除自己的个人数据的权利。且明确如果用户选择行使这些权利，将不会受到区别对待，即用户有权获得与不行使权利时应获得的同等程度的服务质量。同时其隐私政策中还明确了个人信息主体的行权途径以及链接。

此外，其他个人信息主体的权利优秀实现途径如：**用户可对 APP 跟踪权限进行控制，用户可以查看已授权跟踪权限的 APP，更改偏好设置，禁止 APP 今后征求授权等**。随着《个人信息保护法》颁布实施，个人信息主体权利的范围有所扩大，但具体的落地实践方式仍在探索中，例如由于无法准确理解复制权等的

具体操作方式，部分企业自行设计了“导出权”等模式作为自身对用户权利保障的理解。这种探索无疑大胆且有益，是典型的通过技术保障个人信息权利实现的表现。

B.2. 安全责任

B.2.1. 安全保障措施

某手机厂商在隐私政策中披露了其采取的安全保障措施，包括使用技术手段对服务进行加密，对访问个人信息的人员进行限制，保障个人信息安全并实施存储和传输全程安全加密，采用加密传输和存储特殊类型个人信息，严格筛选业务合作伙伴和服务提供商，举办安全和隐私保护培训课程测试与宣传活动，采用国际及业内认可的标准并积极通过相关安全与隐私保护认证等措施。

在安全与隐私保护功能概述中，该厂商表示其将这种 PbD(数据保护和隐私保护嵌入产品设计)理念融入了产品设计的全流程中，并针对浏览器、账户管理、云服务、软件商店、设备系统安全、敏感信息保护等主要业务功能的安全保障措施进行了详细说明。其中，基于信任设备的权限隔离、数据存储加密三层防护机制和敏感操作提醒等。

B.2.2. 数据安全体系

某通讯厂商通过 SRM 机制实现对个人信息的隐藏加密处理。根据官网发布的 PbD 白皮书显示，其通过数据流图 (DFD) 分析来确定数据存储位置、数据流向其他国家和能够访问个人数据的各方，包括目的或用例。其产品功能、个人信息安全保障与隐私和数据保护文档制作分散设置为产品研发组织的职责，而产品安全服务则由专门的安全服务组织负责。

SRM 是一个能够实现安全和隐私目标的框架。它的主要特点是：

- 定义产品安全性和隐私的理想水平
- 确保实施适当的安全和隐私功能
- 跟踪和测量当前产品安全和隐私状态
- 支持创建与产品相关的安全服务

某科技企业在报告中披露了 AI 安全和隐私保护治理实践，其强调“在流程与产品中嵌入要求”，即在产品设计、开发及交付全生命周期，嵌入安全可控的性能指标要求和隐私影响评估要求的控制点，将安全与隐私置于战略优先地位。在此基础上，其在报告中声明将基于不同业务领域的特点，设置差异化的隐私保护目标，并将隐私保护要求嵌入端到端的产品研发流程，要求所有产品版本依此执行。

B.3. 特殊处理

B.3.1. 儿童数据

某手机厂商对儿童数据进行了严格保护。在账户创建阶段，如果未经父母或监护人的许可和同意，13

周岁以下儿童（年龄因地区而异）无法自行创建个人账户。只有其监护人才可以为儿童建立专门的儿童账户并实现对该账户信息、购买行为的控制。

而在用户申请创建儿童的应用商店账户时，该厂商**要求验证用户当前的付款方式**。根据具体付款方式，可能会使用信用卡的安全码或类似的验证方式完成验证。**其要求用户完成验证的目的是，使得验证用户作为家庭组织者的身份并获得用户对收集子女个人信息的同意**。此外，该厂商对儿童信息的使用有着更严格的限制，例如针对儿童的个性化推荐按钮始终处于关闭状态且用户无法开启，针对儿童的“允许 APP 请求跟踪”设置处于关闭状态且无法启用。

某儿童在线教育产品服务提供商隐私政策的内容，除了同样适用于未成年人并对如何保护儿童个人信息进行说明外，还**制定了专门的《儿童隐私保护指引》作为《隐私和数据保护政策》的组成部分**。在首次打开 App 时也会弹窗提示用户阅读，为了确保由监护人阅读理解隐私政策，用户点击隐私政策时还需通过专门的家长验证功能。

B.3.2. 老年人数据

某手机厂商出于保障老年人健康的目的，开发了与家人共享健康数据的功能。该功能允许用户与其他人分享他们的健康数据，这些数据出自不同来源——心率应用程序、血压监测系统等。健康数据共享对于可能想要或需要跟踪老年人的健康指标的家庭成员和护理人员来说非常便利，但同时涉及个人敏感信息收集、处理和共享问题。

为此，该厂商**将该功能完全交由用户控制，用户可以在应用程序中自助决定他们想要共享哪些信息以及谁共享，并始终拥有更改、停止、删除这些信息的权利**。在更好服务老年人的同时，保障老年人隐私和数据保护安全。

参考文献

- [1] 周杨, 江智茹, “隐私保护设计 (PbD): 个人信息保护的学霸方法论”,
<https://mp.weixin.qq.com/s/jbJPpUsMRz73sxvAUyRBnw>, 2021 年 11 月 22 日访问.
- [2] 郑志峰. 通过设计的个人信息保护[J]. 华东政法大学学报, 2018, 21 (06) :51-66.
- [3] [美] 劳伦斯·莱斯格:《代码 2.0: 网络空间中的法律》, 李旭、沈伟伟译, 清华大学出版社, 2018 年, 第 6 页。
- [4] Lisa M. Austin, “Reviewing Pipeda: Control, Privacy and the Limits of Fair Information Practices”, Canadian Business Law Journal, Vol.44, No.1, 2006, pp.21-53.
- [5] Susan Landan, “Control Use of Data to Protect Privacy”, 347 Science Issue 504, 2016.
- [6] Fred H. Cate, “The Failure of Fair Information Practice Principle”, in Jane K. Winn ed., Consumer Protection in the Age of the ‘Information Economy’, Routledge, 2006, pp.356-357.
- [7] Demetrius Klitou, “Privacy by Design and Privacy-Invasive Technologies: Safeguarding Privacy, Liberty and Security in the 21ST Century” 5 (3) Legisprudence 297-298 (2011) .
- [8] Alexandra Rengel , “Privacy-Invasive Technologies and Recommendations for Designing a Better Future for Privacy Rights”, Intercultural Hum. Rts. L. Rev. 224-229 (2013) .
- [9] Batya Friedman, Peter H. Kahn, Alan Borning & Alina Hultgren, Value, “Sensitive Design and Information Systems”, In Neelke Doorn, Daan Schuurbiers, Ibo van de Poel & Michael E. Gorman ed., Early Engagement and New Technologies: Opening up the Laboratory, Springer, 2013, p.56.
- [10] Ann Cavoukian, “Privacy by Design: The Definitive Workshop. A foreword by Ann Cavoukian”, Ph.D, 3 Identity in the Information Society, 2010, p.248.
- [11] Ann Cavoukian, “Privacy by Design: The 7 Foundational Principles”, <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>, 2021 年 11 月 22 日访问。
- [12] Ann Cavoukian, Privacy by Design, Information and Privacy Commissioner, Ontario, Canada, 2013, p. 1.
- [13] Ira S. Rubinstein & Nathaniel Good, “Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents” 28 Berkeley Tech. L. J. 1335 (2013) .
- [14] Kalam & Thierry Sans eds, ICT Systems Security and Privacy Protection, Springer, 2014, pp.51-52.



合规创造价值

Compliance Creates Value

主编：高瑞鑫、宋伟强、杨宇鑫、丁沛、李琳、周杨、杨玥祺、梁天翔、黄惠娥

参编：徐敏、梅傲婷、周宇心、王晨、王志宇、魏安迪、方圆、岳艳红、胡志强、陈正伟、鲁可兴、林峻、惠兆帅、曲绅维、文华龙、蓝友辉、徐艳军

声明：

本文档作为隐私保护设计的研究成果和参考性资料。除非另有约定，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。由于法律和监管环境、标准规范和行业实践不断发展，可对文档内容进行增加、修改、删减、废止，或不定期更新。任何单位和个人不得擅自摘抄、复制本文档的任何内容，应获得授权或注明出处。