产品和服务设计中的消费者隐私保护 第 2 部分：应用案例

1 范围

本文件规定了如何使用 ISO 31700-1 建议，并说明了 ISO 31700-1 应用的案例。

本文件适用于参与开发、实施和运营数字化消费品及服务的工程师和从业人员等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，标注日期的引用文件，仅该日期对应的版本适用于本文件。不标注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

ISO 31700-1 产品和服务设计中的消费者隐私保护 第1部分：高阶要求

3 术语和定义

下列术语和定义适用于本文件。

ISO 和 IEC 在以下地址维护用于标准化的术语数据库：

——ISO 在线浏览平台： 可在 https://www.iso.org/obp 获得；

——IEC 电子百科： 可在 https://www.electropedia.org/ 获得。

3.1

隐私设计 privacy by design

在涉及个人身份信息的产品或服务的初始设计阶段和整个生命周期中应考虑隐私的设计方法，包括考虑产品废弃和删除任何相关的个人身份信息。

注：生命周期还包括更新改造期间。

[来源：ISO 31700-1:2023，3.5]

3.2

应用案例 use case

描述消费者和消费品之间的相互关系，用于帮助识别、梳理和满足需求以支持特定的业务目标。

注 1： 消费者可以是系统的用户和工程师。

注 2：本文件中涉及的系统是消费品或服务。

[来源：ISO 31700-1:2023，3.22，有修改]

4 缩略语

下列缩略语适用于本文件。

NIST：美国国家标准技术研究所

PII：个人身份信息

5 基本要求

5.1 ISO 31700-1 标准要求

ISO 31700-1 规定的具体要求如下（见表 1）：

——通则；

——消费者沟通要求；

——风险管理要求；

——开发、部署和操作设计的隐私控制；

——个人身份信息生命周期结束要求。

表 1 ISO 31700-1 标准要求

类别	章节编号和要求
通则	4.2 设计消费者行使隐私权的功能
	4.3 开发确定消费者隐私偏好的功能
	4.4 为隐私设计人机界面
	4.5 分配相关角色和权限
	4.6 建立多功能职责
	4.7 培养隐私知识、技能和能力
	4.8 确保了解隐私控制
	4.9 文件化信息管理
消费者沟通要求	5.2.提供隐私信息
	5.3 提供隐私信息的责任
	5.4 回应消费者询问和投诉
	5.5 与不同消费者群体进行沟通
	5.6 数据泄露沟通
	6.2 进行隐私风险评估

风险管理要求	
	6.3 评估第三方的隐私能力
	6.4 制定与记录隐私控制要求
	6.5 监测和更新风险评估
	6.6 将隐私风险纳入网络安全弹性设计
开发、部署和操作设计的隐私控制	7.2 将隐私控制的设计和操作应用到产品开发和管理生命周期中
	7.3 设计隐私控制
	7.4 实施隐私控制
	7.5 设计隐私控制测试

	7.6 管理隐私控制的过渡
	7.7 管理隐私控制的运行
	7.8 准备和管理隐私泄露
	7.9 在个人身份信息生命周期中为所依赖的流程和产品操作实施隐私控制
个人身份信息生命周期结束要求	8.2 设计退出和终止使用的隐私控制

5.2 相关概念

本文件 5.1 中各项要求可与以下属性相关联：

——生命周期流程，见表2；

——隐私保护目标，见表 3；

——NIST 隐私框架，见表 4；

——NIST 隐私工程目标，见表 5。

由此产生的关联结果见表 6。

表 2 生命周期流程

组织政策	组织为定义和维护与隐私相关的政策而开展的活动
产品设计与开发	组织为设计和开发消费品或服务而开展的活动
产品用途	组织在使用消费品或服务时为管理隐私而开展的活动

表 3 隐私保护目标

不可链接性	确保个人身份信息主体可多次使用资源或服务且其他主体无法将其相关联
透明性	确保所有与隐私相关的数据处理，包括法律、技术和组织设置，都能被理解和重建
可干涉性	确保个人信息主体、控制者、处理者及监管机构均可干预所有与隐私相关的数据处理

表 4 NIST 隐私框架

识别-P	培养组织对数据管理过程中个人隐私风险的理解
管理-P	制定和实施组织治理结构，以便持续了解由隐私风险提供的组织风险管理优先级

控制-P	制定和实施适当的活动，使组织或个人能够以足够的颗粒度管理数据，从而管理隐私风险
沟通-P	制定和实施适当的活动，使组织或个人能够对数据处理方式和相关隐私风险有可靠的理解并参与对话
保护-P	制定和实施适当的数据处理保障措施

表 5 NIST 隐私工程目标

可预测性	个人、所有者和操作人员能够对数据及其系统、产品或服务的处理进行可靠假设
可管理性	提供数据颗粒度管理功能，包括更改、删除和选择性披露
无关联性	使数据或事件的处理无法与超出系统操作要求的个人或设备相关联

表 6 ISO 31700-1 要求与属性

需求类别	ISO 31700-1 要求	生命周期流程	隐私保护目标	NIST 隐私框架	NIST 隐私工程目标
通则	4.2 设计消费者行使隐私权的功能	产品设计与开发	可干涉性 透明性	控制-p 沟通-p	可预测性 可管理性
	4.3 开发确定消费者隐私偏好的功能	产品设计与开发	透明性	控制-p 沟通-p	可预测性
	4.4 为隐私设计人机界面	产品设计与开发	透明性	控制-p 沟通-p	可预测性 可管理性
	4.5 分配相关角色和权限	组织政策	-	沟通-p	可管理性
	4.6 建立多功能职责	组织政策	-	管理-p	可管理性
	4.7 培养隐私知识、技能和能力	组织政策	-	管理-p	可管理性
	4.8 确保了解隐私控制	组织政策	-	管理-p	无关联性
	4.9 文件化信息管理	组织政策	-	管理-p	可管理性
消费者沟通要求	5.2 提供隐私信息	组织政策	透明性	沟通-p	可预测性
	5.3 提供隐私信息的责任	组织政策	透明性	管理-p 沟通-p	可预测性 可管理性
	5.4 回应消费者询问和投诉	产品用途	透明性	沟通-p	可预测性 可管理性
	5.5 与不同的消费者群体进行沟通	产品用途	透明性	沟通-p	可预测性

	5.6 数据泄露沟通	产品用途	透明性	沟通-p	可预测性
风险管理要求	6.2 进行隐私风险评估	产品设计与开发	不可链接性	识别-p	可预测性 可管理性 无关联性
	6.3 评估第三方的隐私保护能力	产品设计与开发	不可链接性	确定-p 保护-p	可预测性 可管理性 无关联性
	6.4 制定与记录隐私控制要求	产品设计与开发	不可链接性 可干涉性 透明性	识别-p 控制-p 沟通-p	可预测性 可管理性 无关联性
	6.5 监测和更新	产品设计与	不可链接性	识别-p	可预测性

	风险评估	开发		管理-p	可管理性 无关联性
	6.6 将隐私风险纳入网络安全弹性设计	组织政策	不可链接性	识别-p 保护-p	-
开发、部署和操作设计的隐私控件	7.2 将隐私控制的设计和操作应用到产品开发和管理生命周期中	组织政策	不可链接性 可干涉性 透明性	保护-p	可预测性 可管理性 无关联性
	7.3 设计隐私控制	产品设计与开发	不可链接性 可干涉性 透明性	保护-p	可预测性 可管理性 无关联性
	7.4 实施隐私控制	产品设计与开发	不可链接性 可干涉性 透明性	保护-p	可预测性 可管理性 无关联性
	7.5 设计隐私控制测试	产品设计与开发	不可链接性 可干涉性 透明性	保护-p	可预测性 可管理性 无关联性
	7.6 管理隐私控制的过渡	组织政策	不可链接性 可干涉性 透明性	控制-p 沟通-p	可预测性 可管理性 无关联性
	7.7 管理隐私控制的运行	组织政策	不可链接性 可干涉性 透明性	控制-p 沟通-p	可预测性 可管理性 无关联性
	7.8 准备和管理隐私泄露	组织政策	-	保护-p 控制-p	-
	7.9 在个人身份信息生命周期中为所依赖的流程和产品操作实施隐私控制	产品用途	-	控制-p 沟通-p	-

个人身份信息生命周期结束要求	8.2 设计退出和终止使用的隐私控制	产品设计与开发	-	控制-p 沟通-p	可预测性 可管理性 无关联性

5.3 应用案例观点

5.3.1 通则

本文件 5.3 各观点显示在第 7 章应用案例示意图中。

5.3.2 消费品观点

在组织职权范围内，消费品和相关组织应遵循惯例，在产品使用期间及其个人身份信息生命周期中保护消费者隐私。

在产品开发过程中，产品的使用方法需结合不同环境和情况进行评估，以满足用户的不同需求，从而防止理解能力差异较大的消费者在使用产品时不受控制。

对于不同类型的消费品，应准确定义其使用方法，并详细描述与其相关的组织流程，以保护消费者隐私。

消费者对产品的使用可能随时间的推移而变化，并因文化或人口群体而异。

5.3.3 工程框架观点

隐私控制的开发和管理是消费品工程的重要组成部分。由此产生的工程框架结合了以下内容：

——基于 ISO/IEC/IEEE 15288[3]等标准的流程；

——系统生命周期流程；

——扩展此类流程，以整合隐私工程。这些扩展基于 ISO/IEC TR 27550[5]，并在 NIST 隐私框架[7]、OASIS PMRM[6]等框架的指导下实现隐私原则的操作；

——在 ISO 31700-1[1]的指导下整合消费品观点。

5.3.4 生态系统观点

消费品涉及以下两个生态系统：

——供应链，即与系统生命周期过程相关的生态系统。这涉及由第三方提供隐私能力的组织和合同活动；

——数据空间，即与用户和数据提供商相关的生态系统。这涉及数据共享的组织和合同活动。

6 应用案例分析

6.1 通则

应用案例的模板是用一致的方式来说明示例模板的结构，以便所产生的应用案例能够提供关于使用 ISO 31700-1 的例子和理由。

——主要说明的条目是通用的，包括 ID：案例名称；产品、服务或过程的描述；隐私保护目标；感兴趣的生态系统和利益相关系统；用户、股东、个人身份信息、目标以及案例叙述。

——扩展说明的条目遵循 ISO31700-1，包括通用要求、消费通信需求、风险管理要求、发展、设计隐私控制的部署和操作以及个人身份信息生命周期的结束。

6.2 应用案例模板

主要案例分析模板见表 7。

表 7 主要案例分析模板

输入端	应用案例描述
账户	唯一标识
案例名称	名称含义
对产品、服务或过程的描述	产品简介
隐私保护目标	对隐私保护目标的简要描述

生态系统和利益相关系统	描述利益相关系统
用户	描述用户情况
利益相关者	描述利益相关者
个人身份信息	描述所收集的个人资料
目标	描述个人身份信息（PII） 收集的目的
主要叙述	关于消费品和服务的简短叙述

扩展案例分析模板见表 8。

表 8 扩展案例分析模板

输入端	应用案例描述
账户	唯一标识
案例名称	名称含义
补充说明	描述具体的变化，侧重于 ISO3700-1 中某一特定条款的使用。

扩展案例分析类别见表 9。

表 9 扩展案例的要求类别

扩展叙述范畴	与 ISO 31700-1 的联系
通用要求	见 ISO 31700-1:2023,4.2 到 4.9
消费者沟通需求	见 ISO 31700-1:2023,5.2 到 5.6
风险管理需求	见 ISO 31700-1:2023,6.2 到 6.6
开发、部署和操作设计的隐私控制	见 ISO 31700-1:2023,7.2 到 7.9
个人身份信息生命周期结束的需求	见 ISO 31700-1:2023,8.2

7 应用案例

7.1 通则

该部分描述了三个案例：在线零售、健身公司和智能锁。这些案例涵盖了 ISO 31700-1 的要求，如表 10 所示。

注：为每个叙述提供了一个序列图，图 1 到图 16 的的代码可从 https://standards.iso.org/iso/tr/31700/-2/ed-1/en/获取。

表 10 案例需求范围

需求类别	ISO 31700-1 要求		在线零售	健身舞团	智能锁
通则	4.2	4.2 设计消费者行使隐私权的功能	×		
	4.3	4.3 开发确定消费者隐私偏好的功能	×		
	4.4	4.4 为隐私设计人机界面	×		
	4.5	4.5 分配相关角色和权限	×		
	4.6	4.6 建立多功能职责	×		
	4.7	4.7 培养隐私知识、技能和能力	×		
	4.8	4.8 确保了解隐私控制	×		
	4.9	4.9 文件化信息管理	×		
消费者沟	5.2	5.2.提供隐私信息		×	×

通要求	5.3	5.3 提供隐私信息的责任		×	×
	5.4	5.4 回应消费者询问和投诉	×	×	×
	5.5	5.5 与不同消费者群体进行沟通	×	×	×
	5.6	5.6 数据泄露沟通	×		×
风险管理要求	6.2	6.2 进行隐私风险评估	×	×	×
	6.3	6.3 评估第三方的隐私能力	×	×	×
	6.4	6.4 制定与记录隐私控制要求	×	×	×
	6.5	6.5 监测和更新风险评估	×	×	×
	6.6	6.6 将隐私风险纳入网络安全弹性设计			×
开发、部署和操作设计的隐私控制	7.2	7.2 将隐私控制的设计和操作应用到产品开发和管理生命周期中			×
	7.3	7.3 设计隐私控制	×		×
	7.4	7.4 实施隐私控制	×		×
	7.5	7.5 设计隐私控制测试			×
	7.6	7.6 管理隐私控制的过渡			×
	7.7	7.7 管理隐私控制的运行	×		×
	7.8	7.8 准备和管理隐私泄露	×		×
	7.9	7.9 在个人身份信息生命周期中为所依赖的流程和产品操作实施隐私控制	×		×
PII 生命周期结束的要求	8.2	8.2 设计退出和终止使用的隐私控制	×		

7.2 在线零售

7.2.1 在线零售使用案例主要描述

账户	唯一标识	案例 31700-01a
应用案例名称	名称含义	在线零售
产品、服务或流程的描述	产品简介	一种允许客户通过互联网远程搜索、选择和购买产品、服务和信息的服务。

隐私保护目标	对隐私保护目标的简要描述	确保零售商提供或收集的个人信息于仅限用于完成销售、交货、提供收据和支持。
利益系统和相关系统	描述利益相关系统	客户隐私期望 客户购买后的隐私期望 在线零售商交易系统 在线零售商的订单履行信息系统 在线零售商的送货系统 互联网服务供应商信息系统
用户	描述用户情况	消费者下单
利益相关者	描述利益相关方	零售商配送人员 订单处理系统

		送货系统 支付系统 退货系统 营销和跟踪系统 消费设备(如平板电脑、智能手机、笔记本电脑)
个人身份信息	描述收集的个人身份信息	客户姓名、地址、电子邮件和电话； 用于处理支付订单的信用卡信息。
产品使用目的	描述收集个人信息的目的	卖方手机个人身份信息是为了完成订单、促进产品开发和服务改进。
主要说明	关于消费品和服务的简短叙述	一位消费者上网为孙辈寻找玩具。在查看了多个网站和一些他尚未完成的订单后，消费者通过一个在线零售商处理了2个订单。为了完成订单，他提供了包括送货地址和付款方式在内的联系信息。为了运输和订购，他提供了自己的联系信息和地址。为了付款，他输入了自己的信用卡。在线零售商询问他是否想要创建一个账户，他拒绝了。在线零售商询问他是否希望他们在发货后保留联系信息，以便将来购买或退货。除了与退货有关的，客户拒绝允许这样做。在线零售商还询问了一些关于家庭规模、年龄和收入的问题。客户拒绝回答，并拒绝接受任何有关新产品的信息。

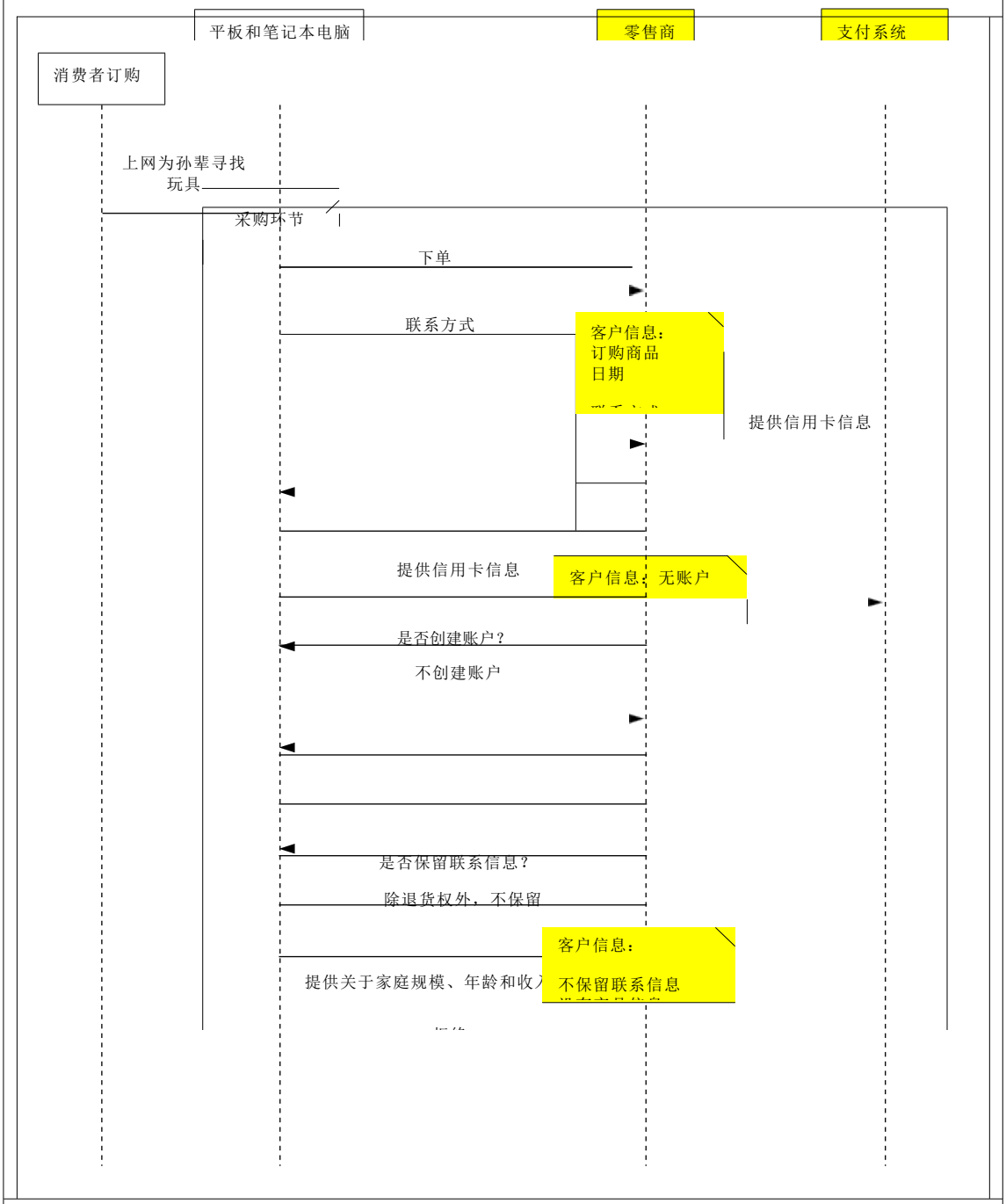

图 1 在线零售使用案例主要描述示意图

7.2.2 在线零售消费者沟通

账户	唯一标识	案例 31700-01b
使用案例名称	名称含义	在线零售

关于消费者沟通的说明	描述消费者沟通的需求如何提供帮助	零售商公司的信息系统受到网络安全攻击，导致系统停止运行数小时。 该组织启动了其消费者支持计划，在网上发布隐私声明，确认不存在隐私泄露。 客户对其购买的产品进行具体询问，并获得定制信息，使其确认他的订单、付款及个人信息没有受到影响。

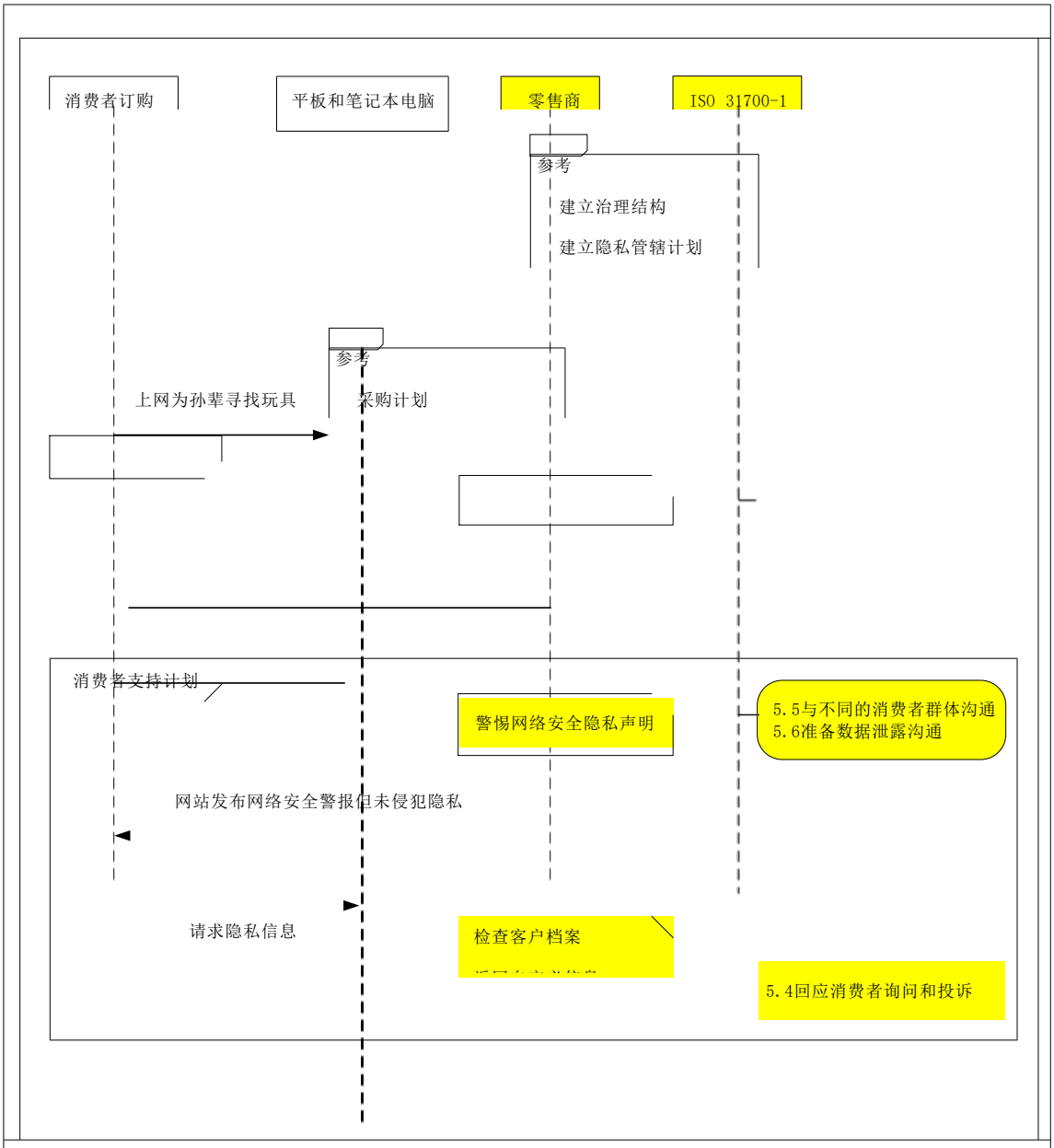

图 2 在线零售消费者沟通示意图

7.2.3 在线零售概述

账户	唯一标识	案例 31700-01c
使用案例名称	名称含义	在线零售

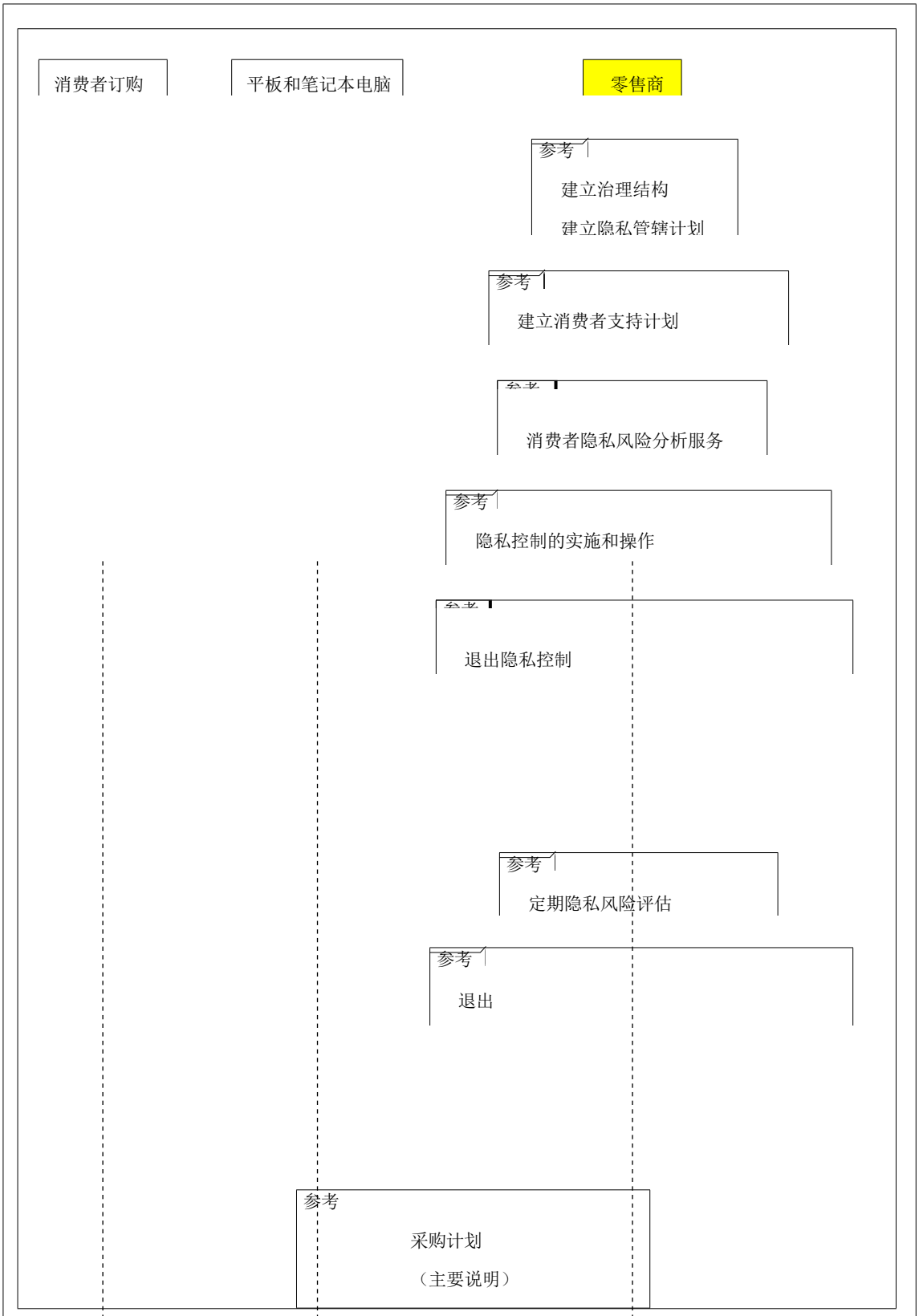

图 3 在线零售概述示意图

7.2.4 在线零售基本要求

账户	唯一标识	案例 31700-01d
使用案例名称	名称含义	在线零售
关于基本要求的说明	描述基本要求如何提供帮助	一家公司想创建一个在线零售业务。该公司通过建立治理结构来处理隐私合规和消费者沟通问题，并进一步为从事整个数据处理生态系统的员工建立隐私管辖计划，涉及法规和隐私增强技术的知识。公司还创建了消费者支持计划，包括消费者在隐私方面的互动能力。

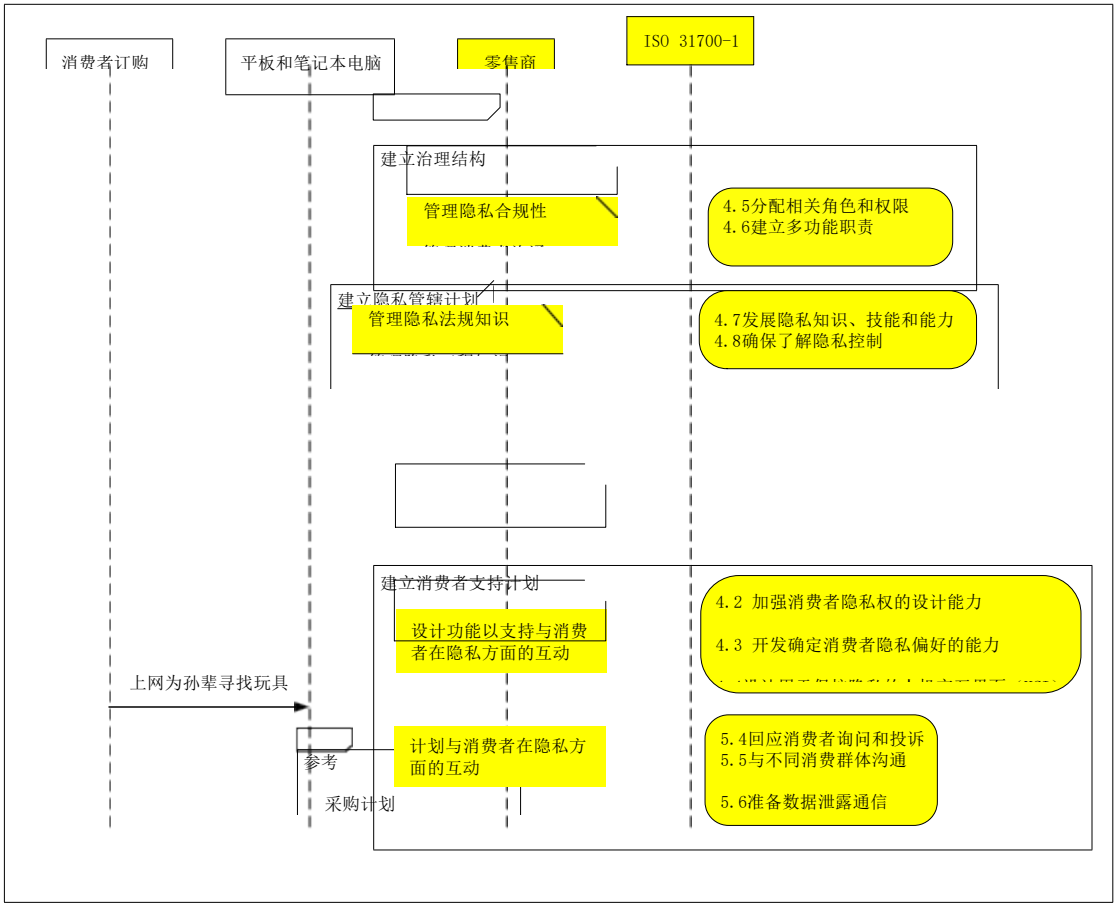

图4 在线零售基本要求示意图

7.2.5 在线零售风险管理

账户	唯一标识	案例 31700-01e
使用案例名称	名称含义	在线零售
关于风险管理的说明	描述风险管理如何帮助	零售商的产品管理团队进行初步的消费者服务隐私风险分析，从而提出消费者支持要求和数据存储保护要求。对提供数据存储保护的供应商进行评估后，可选择实施。

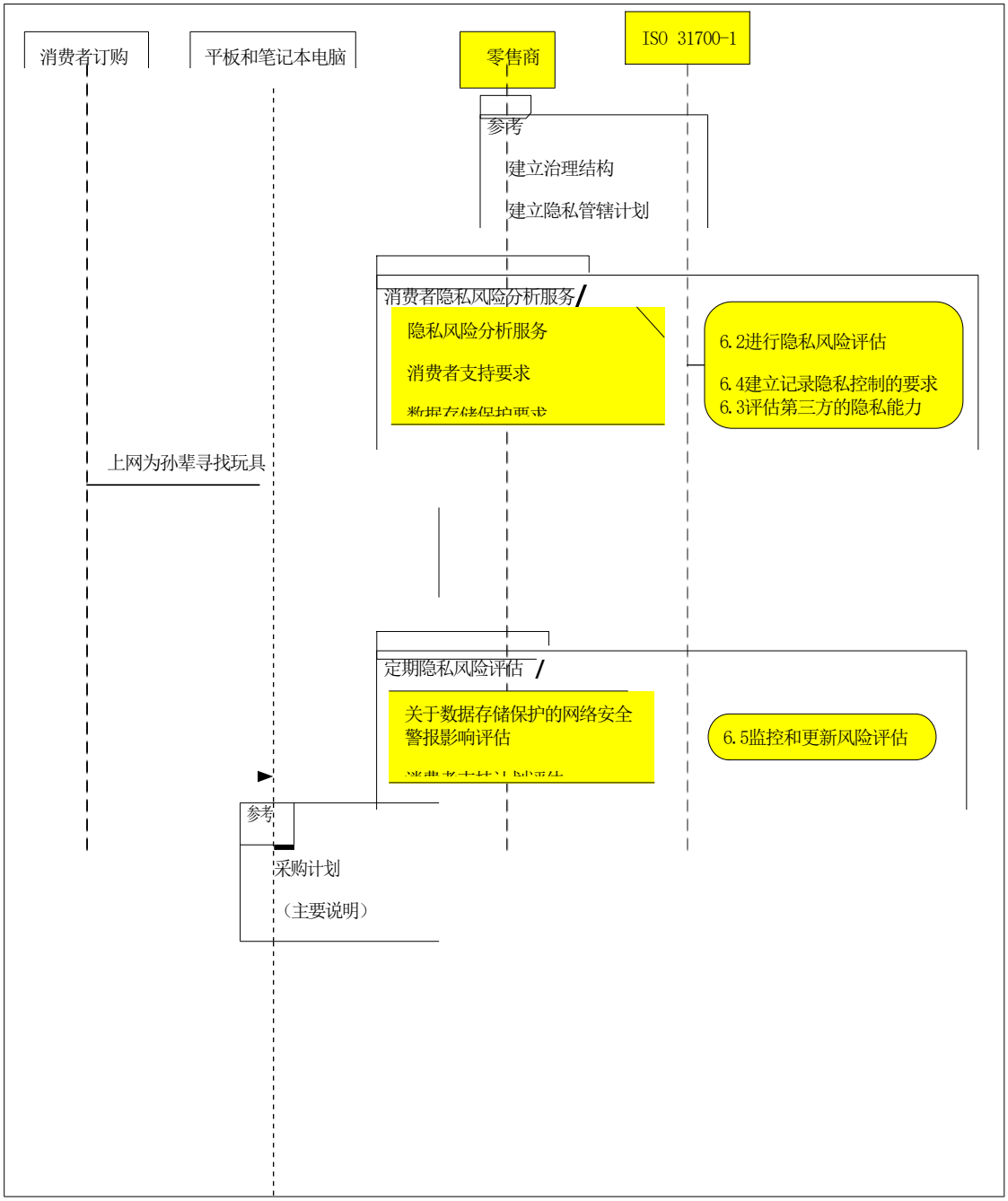

图5 在线零售风险管理示意图

7.2.6 在线零售开发、部署和操作

账户	唯一标识	案例 31700-01f
使用案例名称	名称含义	在线零售

关于开发、部署和操作的说明	描述对隐私控制的要求如何帮助	除消费者隐私风险分析服务外，开发团队还被授权对消费者账户实施隐私控制，其中包括访问控制政策执行和监测机制，以及相关雇员可以访问数据规则的相关组织措施。