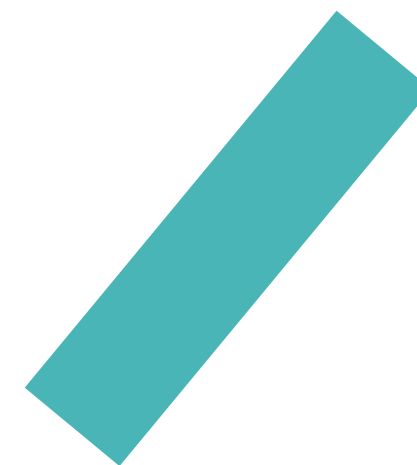




# 得物个人信息保护

## 社会责任报告



# 目录

## 01 前言

## 03 优秀实践

- 3.1 安全认证 /14
- 3.2 得物隐私合规智能检测项目 /16

## 04 结语

## 02 得物个人信息保护框架

2.1 个人信息保护管理	/3
个人信息保护制度	/3
个人信息保护组织建设	/5
知识管理和培训宣贯	/6
审计监督	/7
技术工具	/7
用户权益保护	/9
风险管控与响应	/9
Privacy by Design (PbD)	/10
2.2 全生命周期个人信息保护	/11
2.3 合作方安全管理	/12
2.4 SDK安全合规	/13
2.5 未成年个人信息保护	/13
2.6 产业发展	/14

## 01 前言

作为新一代品质生活购物社区，得物 App 以正品电商和品质生活社区作为两大核心服务。成立十年来，它始终致力于帮助用户得到美好生活，已成为年轻用户重要的潮流阵地与品质生活购物平台。

得物在坚持严格的选品标准、专业的查验鉴别、统一的履约交付等服务的同时，尊重和保护个人信息，并不断完善个人信息保护建设，《得物个人信息保护社会责任报告》将公开展示得物在个人信息保护建设所做的持续努力，为用户提供更安全放心的服务和购物体验。

## 02 得物个人信息保护框架

得物通过建立一个全面、持续、有效的隐私保护框架，以确保个人数据的安全和合规处理，并赢得用户和利益相关者的信任。同时明确个人信息保护建设的愿景，建立保护用户个人隐私权益、遵守法律法规、赢得用户信任的高效、透明的管理体系。

愿景：尊重和保护用户隐私，为用户提供更安全放心的服务和购物体验。如图2-1所示。

2.1 个人信息保护管理

(1) 个人信息保护制度

■ 制度体系搭建、洞察跟踪

得物在进行个人信息保护管理时，通过对法律法规和监管政策的研究解读，结合公司实际需要，制定符合业务的制度规范以及建立对应的合规流程。

在隐私保护与治理的过程中，持续对新的隐私保护要求以及行业规定进行识别和集成，紧密跟进个人信息处理相关的法律法规、业界标准和行业实践，及时更新隐私管理制度、流程和实践以应对变化。以保证在稳固底座之上建立具备兼容性、可扩展性且符合企业实际情况的控制要求。建立合规监管机制，包括周期性跟进要求、完善内部制度和流程、积极整改问题、有效响应和评估改进效果。

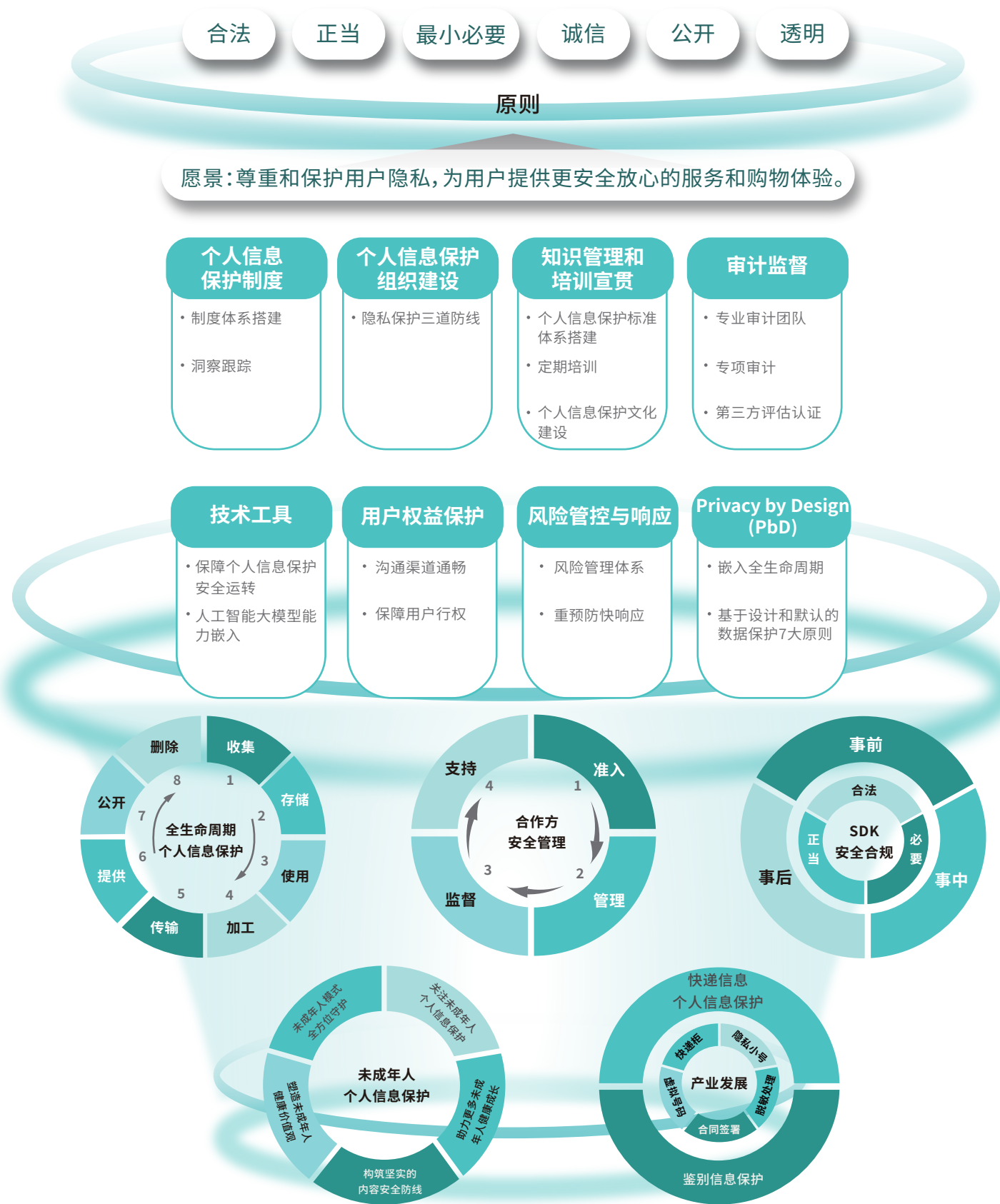


图2-1 得物个人信息保护框架

(2) 个人信息保护组织建设

■ 隐私保护三道防线

得物设立信息安全委员会、数据安全委员会，并确立个人信息保护负责人，保障公司的信息安全、数据安全，个人信息保护战略与规划在组织层面有效落地。通过设置个人信息保护管理的三道防线，明确各方职责分工，统筹推进个人信息保护工作的实际运行。如图2-2所示。

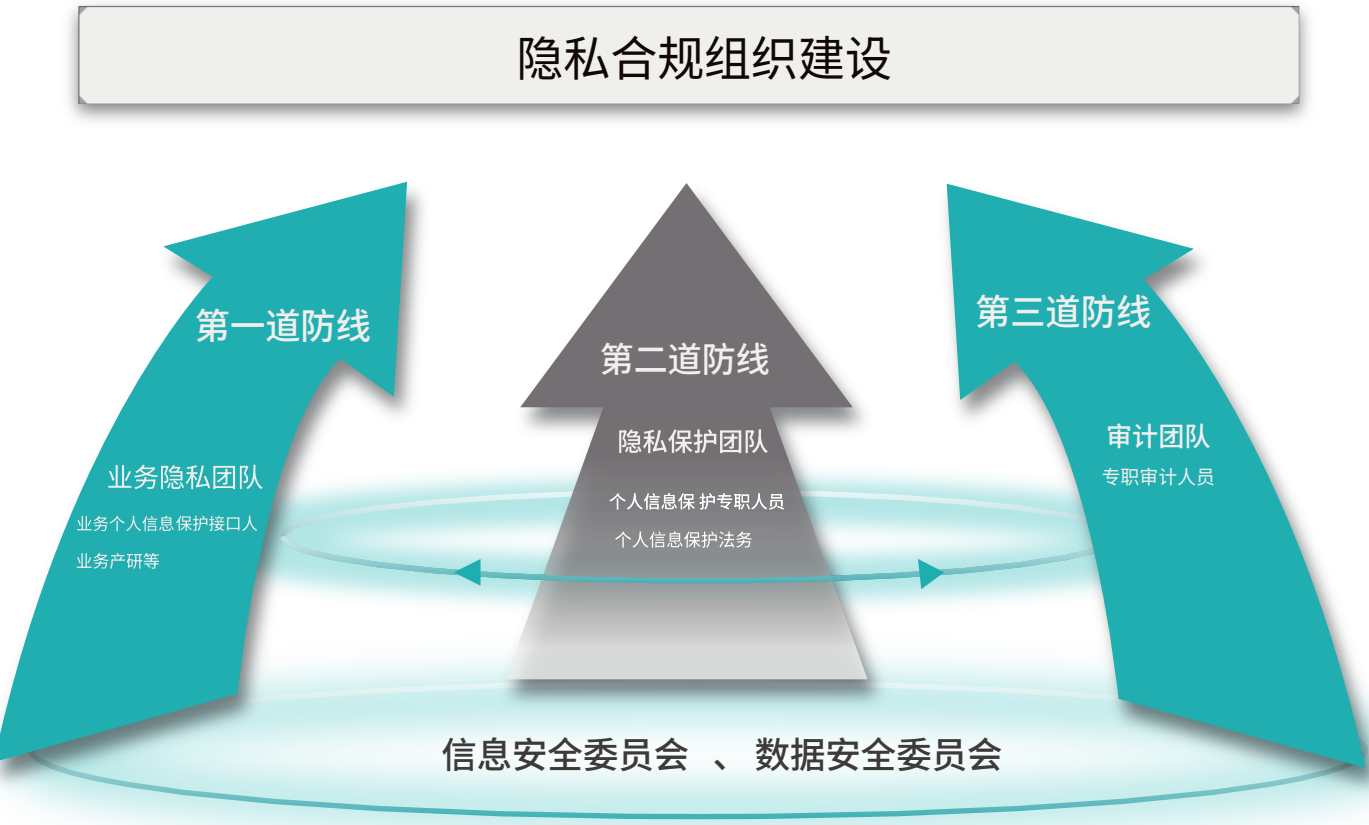


图2-2 隐私合规组织建设

【业务隐私团队-业务个人信息保护接口人、业务产研等】第一道防线，由各业务部门负责隐私保护职能的团队，负责业务产品的隐私设计以及隐私策略的落地，并持续开展自查自纠工作。

【隐私保护团队-个人信息保护专职人员、个人信息保护法务】第二道防线，由专职的个人信息保护职能团队，解决共性问题，负责个人信息保护的建设和支持。

【审计团队-专职审计人员】第三道防线，独立的审计团队，负责业务产品隐私设计以及隐私策略落地的审计，发现并推动风险整改。

(3) 知识管理和培训宣贯

■ 个人信息保护标准体系搭建、定期培训、个人信息保护文化建设

得物重视个人信息保护知识体系的搭建以及合规知识培训。

密切关注监管动向、合规趋势、处罚案例、行业热点等信息，由专业个人信息保护标准团队进行内部标准的制定和丰富，形成外规内化的标准沉淀机制，持续丰富个人信息保护标准体系，成为未来新功能合规落地的重要环节。

定期开展多层次、多维度的个人信息保护相关的意识提升、教育培训、岗位考试、案例分享等多样活动，制定年度培训目标与计划。同步更新培训台账，记录培训考试覆盖人次、时长等信息。

持续性的开展个人信息保护文化宣贯，通过工区海报、会议室投屏、系统登录界面banner轮播等线上线下多渠道覆盖，提高全体员工的个人信息保护意识，营造个人信息保护文化氛围。



(4) 审计监督

专业审计团队、专项审计、第三方评估认证

为满足监督和审计要求，开展业务部门自查，审计团队有效识别用户个人信息管理风险，提出整改建议并推进整改方案落地，满足监管层面合规，同时提升内部管理水平，降低合规风险。定期开展对涉及个人信息处理的信息系统、人员等的专项审计，对个人信息保护评估意见的落地情况进行审计。

得物连续多年获得ISO/IEC 27001:2022信息安全管理体ISO/IEC27701:2019隐私信息管理体系双认证，通信网络安全防护管理三级，信息系统安全等级保护三级认证，满足国际相关法律和制度要求，全面履行和落实网络信息安全责任义务。同时，积极与监管机构、行业协会和科研机构合作，通过协同联动的方式，共同努力构建坚固的信息安全保护屏障，从而构建“企业自查+第三方审计+行政监管”的三层治理体系。

(5) 技术工具

保障个人信息保护安全运转、人工智能大模型能力嵌入

得物结合业务实际情况，合理协调隐私运营、基础安全、安全运营与技术工具的关系，保障个人信息保护安全运转，确保产品和服务在数据处理活动中始终符合个人信息保护的要求。运用人工智能大模型结合实际经验，开发自动化测试工具，旨在提升个人信息保护管理水平。通过智能算法快速生成个人信息保护的测试用例，从而提高测试的效率和准确性。实施全链路监测，实时追踪敏感API的调用和数据传输并提供预警及时识别合规风险。针对异常行为迅速做出响应，形成有效的风险管理闭环。如图2-3所示。

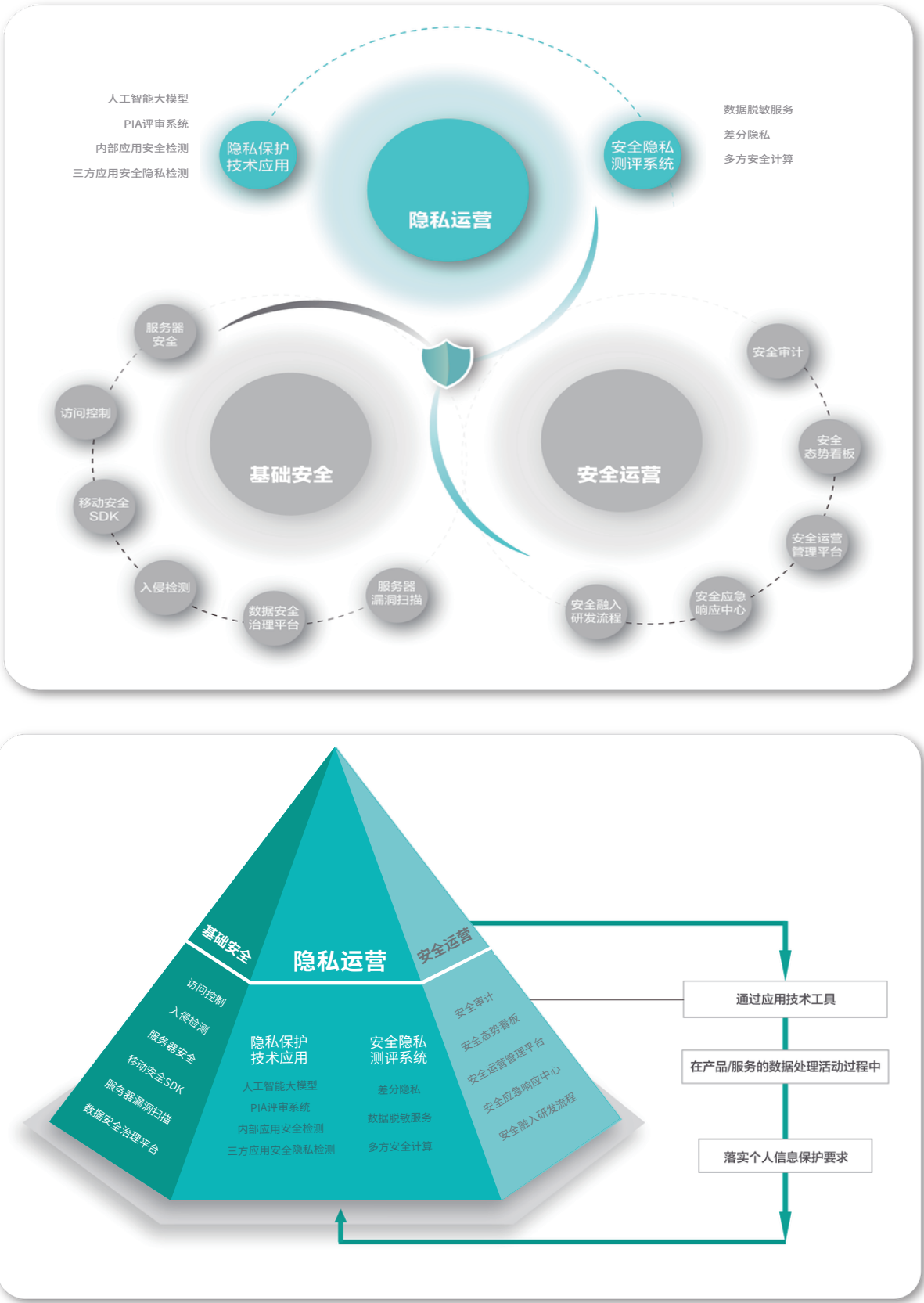


图2-3 隐私合规技术工具

(6) 用户权益保护

沟通渠道通畅、保障用户行权

得物尊重和保护用户隐私，用户在使用得物期间，享有个人信息权益，包括便捷地查阅、复制、更正、删除个人信息，同时保障用户撤回对个人信息处理的同意及注销帐号的权利。

此外，得物还设置了投诉举报、请求解释的渠道，保证用户的意见及请求得到及时响应和处理。针对个人信息保护方面，对用户反馈事项进行详尽的收集、统计、分析、处理，配备专门的合规团队负责个人信息权益请求响应渠道的管理和运营，确保按照相关的合规要求响应。满足不同用户群体的个性化需求和特殊权益保护，制定多种不同的方案和措施（例如未成年人模式、学生身份认证等）。开发和应用相关技术，对于收集的信息，采取符合业界标准的安全防护措施保护用户信息，以防止信息的泄露、丢失、不当使用、未经授权访问、修改和披露等，例如加密技术、去标识化、数据访问权限控制和严格的身份认证等。

同时，得物积极承担企业社会责任，在个人信息保护方面采取积极行动，通过官方渠道向公众展示个人信息保护方面的工作。

(7) 风险管控与响应

风险管理体系、重预防快响应

建立个人信息保护风险管理体系，对涉及个人信息处理的业务活动持续开展隐私风险识别、分析、评价、处置和监控工作。如图2-4所示。

公司根据隐私监测规则进行整体布控，各业务域各司其职开展风险的日常预防工作。制定并持续完善公司应急预案，明确应急处置工作要求，以及监管沟通机制，

定期开展应急响应培训与演练，做好网络安全检查、隐患排查、风险评估和容灾备份工作，避免或减少安全事件的发生及危害，提高应对信息安全事件的能力。

根据实际发生的风险事件，依据制度和流程立即妥善处置，并对于已经发生的事件开展复盘和总结工作，采取相关改进措施避免类似事件再次发生。

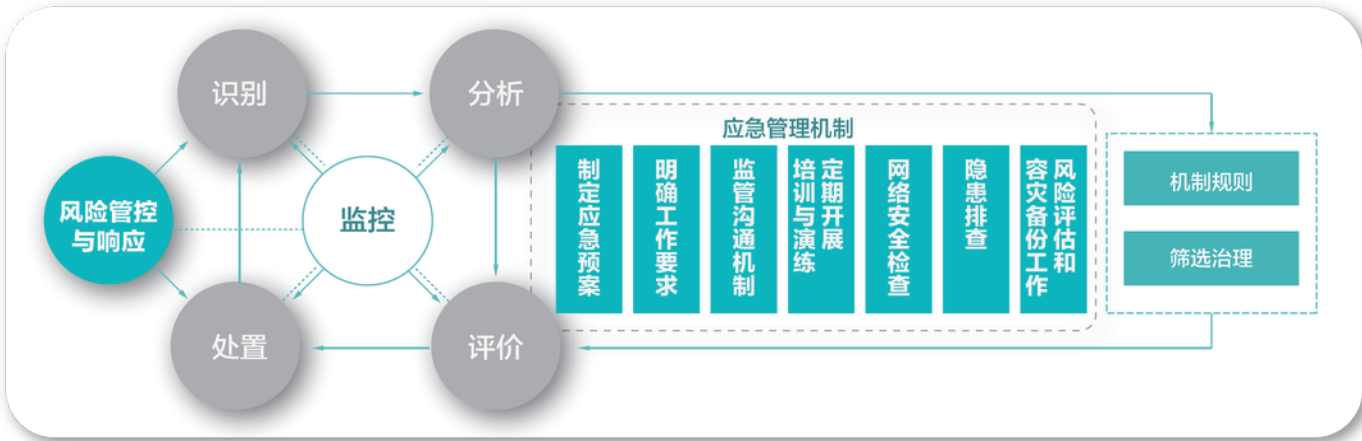


图2-4 得物风险管控与响应

(8) Privacy by Design (PbD)

嵌入全生命周期、基于设计和默认的数据保护7大原则

得物坚持将隐私保护贯穿至产品需求、设计、开发、运营的整个生命周期中，实践 PbD 要求，包括组织内的隐私意识、内部政策、问责措施、对数据主体的透明度，与第三方和数据处理者的合作(包括数据处理协议)，确立开发过程中角色-产出的责任体系，将研发、安全、运营、法务等人员明确于开发链路中。并基于设计和默认的数据保护7大原则，充分体现了以用户为中心的隐私保护宗旨。如图2-5所示。

得物针对涉及个人信息处理的活动设置了PIA（个人信息安全影响评估）流程，检验其合法合规程度，把控其对个人信息主体合法权益造成不利影响的风险，以及评估用于保护个人信息主体的各项措施有效性。内部配套开发并建立供PIA评估人员以



及和业务相关人员使用的系统平台。开发AI自动预评审能力，通过后端定时任务拉取数据，清洗和过滤后提取出待评审需求文件、调用人工智能模型进行智能评估。通过系统能力与AI的高效开展，提升风险覆盖与管控能力，并确保检测效果。

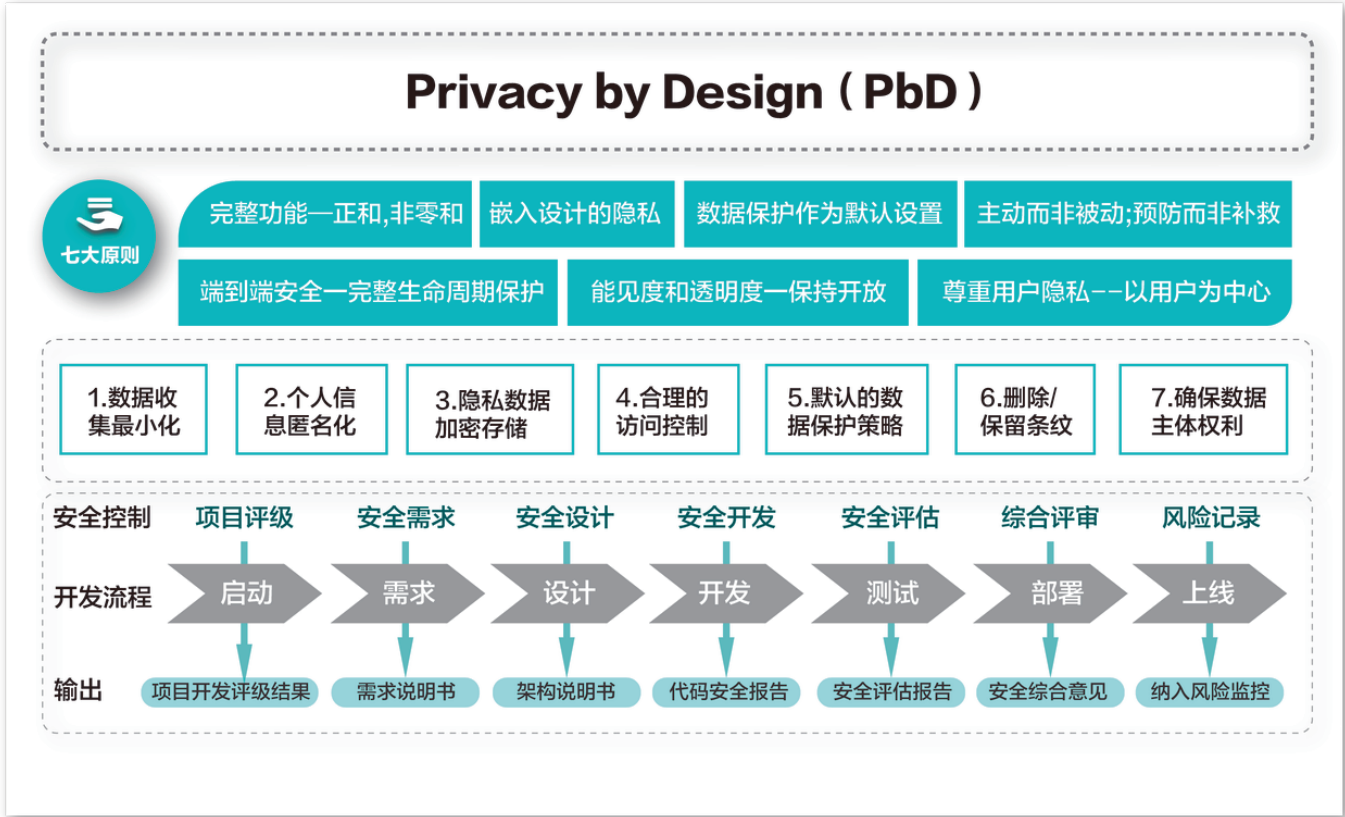


图2-5 Privacy by Design (PbD)

2.2 全生命周期个人信息保护

得物高度重视用户的个人信息安全，为营造安全的购物环境，各业务域采用适当的技术和组织措施保护个人信息。建立起全生命周期保护，从个人信息的事前、事中、事后，全方位落实保护措施，保障全流程管控能力。如图2-6所示。

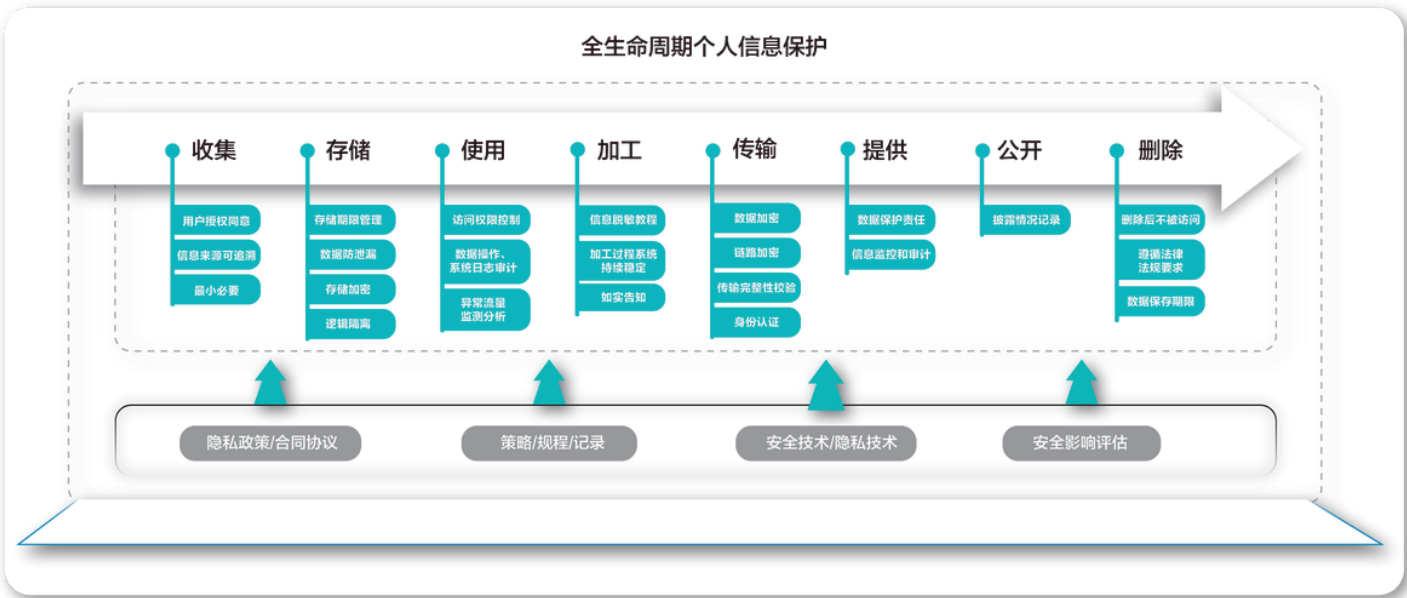


图2-6 全生命周期个人信息保护

2.3 合作方安全管理

得物在涉及公司与合作方建立数据处理合作关系时，通过建立合作方数据安全管理制度对合作方的准入、管理、监督、支持进行了明确要求。对于涉及数据处理、转让、共享等处理活动的合作方进行充分评估，在保证合法合规和服务质量的前提下，优先考虑个人信息保护表现优良的合作方，与合作方签订合作协议，明确其数据安全保障的责任和义务。

合作过程中，基于责任共担、生态共建、互信共赢的理念，持续监督合作方合规情况，建立合作方数据传输监控，确保个人信息在传输、存储、处理、共享等各个环节均得到适当保护。就合作方出现的不合规情况及时处理，必要时采取第三方机构评估、终止合作等合规措施。合作结束时，严格按照合作协议中规定的数据责任和义务，监督合作方及时清除、销毁非必要保留的个人信息。同时，积极推动合作项目的持续发展和共同成长，不断完善合作机制，提供良好的合作环境，共同创造更大的价值。

## 2.4 SDK安全合规

得物始终坚持在合法、正当、必要的原则下接入第三方SDK，通过得物《隐私权政策》及时告知用户并提醒用户关注在涉及到第三方SDK的产品和服务时第三方SDK的用户个人信息处理规则，并在事前、事中、事后采取全方位措施，以保障用户隐私安全。

得物要求第三方SDK应明确告知其所收集使用个人信息的目的、方式和范围，同时要求其做出承诺，其应最小化收集使用个人信息，尽量采取本地方式处理个人信息；并应公开其收集使用个人信息的种类、目的、频次、时机、场景以及触发条件，在满足个人信息收集的合规性原则时，也需满足必要性原则。得物会主动关注SDK风险情况，并对第三方产品或服务进行安全监测，以确保所有接入严格合规。

## 2.5 未成年人个人信息保护

得物一直致力于履行社会责任，关注未成年人的健康成长和个人信息保护。一直以来，坚持落实《未成年人保护法》《未成年人网络保护条例》等法律法规要求，积极落实中央、上海两级网信办的清朗专项，给未成年人提供安全、健康、绿色的网络环境，努力为未成年人的健康成长和信息安全保驾护航。

得物始终高度重视未成年人个人信息保护，通过制定专门的《得物未成年人个人信息保护规则》，采取严格的数据使用和访问制度，确保只有授权人员才可访问，并适时对数据和技术进行安全审计。同时，得物会采取加密措施及其他技术手段存储未成年人个人信息，确保未成年人信息安全。

## 2.6 产业发展

### ■ 快递信息个人信息保护、鉴别信息保护

在当前电商行业用户隐私保护需求日益迫切的背景下，得物作为以正品电商和品质生活社区为两大核心服务的综合平台，得物从自身业务和技术优势出发，携手各利益相关方，持续开展用户信息保护的行动，为个人信息保护建设贡献力量，共同构建一个良好的产业环境，推动产业的创新、竞争力和可持续发展。

为落实用户隐私在快递信息中的个人信息保护安全措施，得物对快递面单中的用户信息进行脱敏处理的隐私保护动作，并通过合同签署方式明确快递供应商的责任与义务；为避免第三方渠道用户信息泄露，推动得物隐私小号服务落地，进一步更好地扩充隐私小号服务商、增加对快递柜的支持、对快递员通过虚拟号短信触达用户的支持，并基于用户体验角度进行充分考虑，在保障消费者个人信息权益的同时，带来放心、安心的服务。

## 03 优秀实践

### 3.1 安全认证

得物致力于建设安全可靠的网络环境，在保障客户端安全、隐私安全、数据安全、内部信息安全、应用安全、网络安全、主机&容器安全等方面上持续获得权威机构肯定，专业性和成熟度处于业内较高水准。连续多年获得ISO/IEC27001:2022信息安全管理体系、ISO/IEC 27701:2019隐私信息管理体系双认证，通信网络安全防护管理三级，信息系统安全等级保护三级认证为年轻人带来可信赖的购物体验。

(1) 信息系统安全等级保护三级认证

信息系统安全等级保护三级认证是《GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求》简称网络安全等级保护，是中国国家标准化委员会发布的信息安全标准，也是目前互联网信息安全管理行业的重要标准。等级根据信息系统的重要程度，从低到高分为一至五个等级，不同安全等级实施不同的保护策略和要求。得物已通过三级信息系统的认证，即非银行机构的最高等级保护认证。

(2) 通信网络安全防护三级认证

通信网络安全防护三级认证是根据《通信网络安全防护管理办法》要求的一项认证工作。得物已获得通信网络安全防护定级（三级）备案证明，展现了完备的通信网络安全防护能力。

(3) ISO/IEC 27001: 2022信息安全管理体系、ISO/IEC 27701: 2019隐私信息管理体系

ISO/IEC 27001: 2022信息安全管理体系作为全球应用最广泛、最权威的信息安全管理标准之一，其对企业隐私保护、数据处理和信息管理等均提出多项高规格的技术和管理标准，是企业安全管理与技术服务先进性、现代化与合规的权威指标。得物已通过此项认证，体现了其在网络基础安全能力和信息安全保障能力上均达到国际高标准。

ISO/IEC 27701: 2019隐私信息管理体系建立在 ISO/IEC27001 要求的基础之上，规定了建立、实施、维护和持续改进隐私相关所特定的信息安全管理体系的要求。得物已通过此项认证，建立起保护个人信息的管理体系（简称 PIMS），将处理个人可识别信息（PII）所需的隐私保护措施纳入考量。

(4) PIA二星级标识认证

得物在第六批“PIA标识”名单 - 个人信息保护影响评估（PIA）专题工作中，获得PIA标识二星级+标识，标志着在个人信息保护与数据治理方面具备了系统化的管理能力和较高标准的合规实践。

3.2 得物隐私合规智能检测项目

得物坚持不断完善技术安全能力，致力于建设安全可靠的网络环境，让用户获得新潮又放心的购物体验。自研合规智能检测管理系统—隐私先锋系统，整合了AI技术与自动化测试能力，由“用例管理平台-Tesla移动端测试体系-合规检测系统”构成，形成闭环管理机制。

通过AI辅助测试用例编写，系统借助智能算法快速生成隐私合规测试用例，显著提高测试效率，保证合规性检测的准确与高效。全链路监测与智能归因，通过全链路监测，可实时追踪敏感API调用及数据传输并进行预警，帮助企业快速识别合规风险。风险监测与响应方面，系统具备多维度数据分析能力，可实时监测异常行为，快速响应合规风险，形成有效的风险管理闭环。

04 结语

得物始终坚持将安全和隐私保护作为重要核心工作，公司自上而下高度重视，从组织建设、产品设计、技术发展和生态搭建等多维度贯彻隐私保护价值观。以“用户中心”为驱动，建立健全全生态、全周期、全流程的隐私保护管理框架。

得物将持续长期投入，在做好数据安全和用户个人信息保护的基础上，积极响应日趋严格的全球化数据合规和隐私保护要求，进一步深入在安全合规领域的各方合作，通过多种安全合规解决方案向用户提供更加安全放心的购物环境，为企业数字化业务稳健运营保驾护航。