KPMG

建立健全个人信息保护管理体系

中华人民共和国个人信息保护法（个保法）

挑战与应对

kpmg.com/cn

个保法要点回顾

《中华人民共和国个人信息保护法》（以下简称“个保法”）经过近两年的筹备，三次审议，于2021年8月20日由十三届全国人大常委会第三十次会议表决通过，将于2021年11月1日起施行。对比一审稿和二审稿，个保法终稿在个人信息处理的合法性基础、个人信息处理者的合规义务、个人信息跨境提供和法律责任等方面均有不同程度的更新。

适用范围

- 在中国境内处理个人信息的活动
- 符合条件的在中国境外处理境内自然人个人信息的活动

个人信息处理者

- 自主决定处理目的、处理方式等个人信息处理事项的组织、个人
- “特殊”的处理者：共同处理，委托和受托处理，第三方等

合法基础

- 取得个人的同意
- 为订立、履行个人作为一方当事人的合同所必需，**或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需**
- **依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息**
- 法定职责或义务履行、应对突发或紧急情况、为公共利益实施新闻报道、舆论监督等行为，法律、行政法规规定的其他情形

合规义务

- 组织人员、制度流程、技术防护等
- 处理敏感个人信息应符合额外要求，**处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则**
- 应受理和处理个人行使权利的申请，进一步约定**个人信息可携带权、自然人死亡后主体权利行使等**
- 事前进行**个人信息保护影响评估，并应定期开展合规审计**

个人信息跨境提供

- 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在境内收集和产生的个人信息存储在境内
- 合法出境条件包括：通过国家网信部门组织的安全评估、按照国家网信部门的规定经专业机构进行个人信息保护认证、**按照国家网信部门制定的标准合同与境外接收方订立合同**，约定双方的权利和义务等
- 事前**个人信息保护影响评估**和单独同意，且**境外接收方处理个人信息的活动达到个保法规定的个人信息保护标准**

法律责任

- 责令整改，没收违法所得，针对组织和人员的罚款，记入信用档案，赔偿损失等
- **对违法处理个人信息的应用程序，责令暂停或者终止提供服务**
- 罚款上限五千万元以下或上一年度营业额百分之五以下
- 对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，**并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人**

中华人民共和国网络安全法（网安法）Cybersecurity Law of the People's Republic of China (CSL)	中华人民共和国数据安全法（数安法）Data Security Law of the People's Republic of China (DSL)	中华人民共和国个人信息保护法（个保法）Personal Information Protection Law of the People's Republic of China (PIPL)
2017年6月1日生效 Enacted June 1st, 2017	2021年9月1日生效 Enact from September 1st, 2021	2021年11月1日生效 Enact from November 1st, 2021

个保法作为个人信息保护的专门法律，应作为个人信息保护工作的主要参考依据，可同比于其他数据保护法案，如欧盟通用数据保护条例、加州消费者隐私法案等

资料来源：毕马威整理

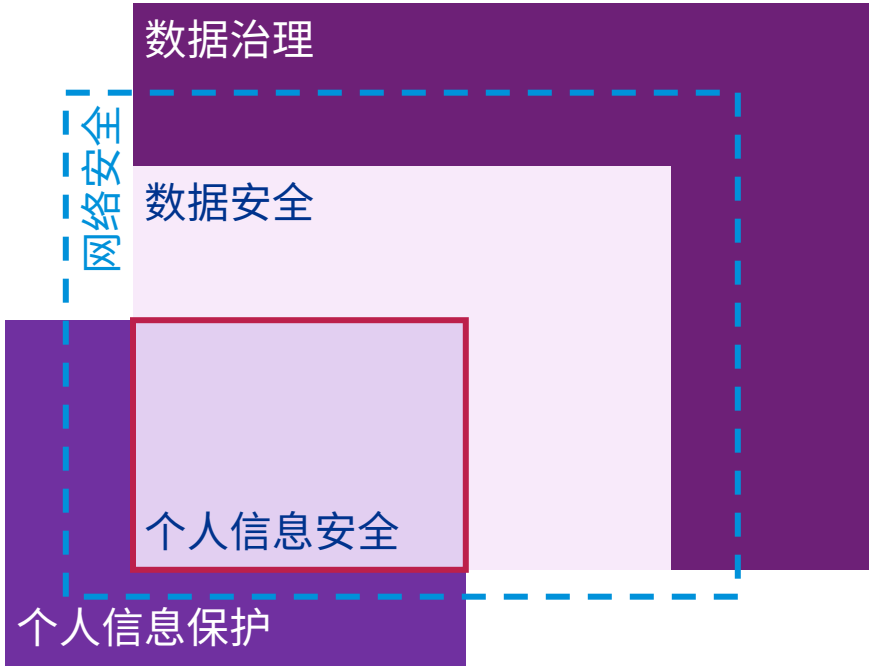
注：粗体部分为个保法终稿部分更新内容小结。

理解企业的多重身份

- 企业基本作为**网络运营者**（网安法），**数据处理者**（数安法）和**个人信息处理者**（个保法）
- 部分企业可能涉及重要数据的处理
- 少数企业可能涉及国家核心数据的处理和（或）关键信息基础设施运营

企业从基本合规义务出发，应建立健全：

1. 信息安全管理体系
2. 数据安全管理体系
3. 个人信息保护管理体系



资料来源：毕马威整理

关联阅读
开展过EU GDPR合规工作的企业还应关注什么？

适用范围	• 个保法适用范围基于个人信息处理活动的地域，而EU GDPR适用范围基于数据所有者及数据处理者的设立地点
个人信息处理者	• 个保法下定义“个人信息处理者”和特殊类型的“个人信息处理者”和EU GDPR下定义“数据所有者”及“数据处理者”稍显不同 • 个保法下敏感个人信息定义略有差异
合法基础	• 个保法覆盖了在合理范围内处理个人自行公开或其他已经合法公开的个人信息 • 个保法明确了按照依法制定的劳动规章制度和依法签订法人集体合同实施人力资源管理所必需 • 个保法对于特定的个人信息处理场景要求获得“单独同意”
合规义务	• 个保法隐私声明内容要求略有差异 • 个保法要求处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则 • 个保法规定的个人信息主体权利略有差异，尤其是个人有权要求个人信息处理者对其个人信息处理规则进行解释说明、自然人死亡后主体权利的行使 • 个保法要求对个人信息进行分类保护 • 个保法要求的个人信息保护影响评估的启动条件和记录保存时长略有差异 • 个保法对APP收集个人信息、“大数据杀熟”、公共场所图像采集等制定了针对性处理规则 • 个保法要求在境内开展分析、评估境内自然人的行为的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表
个人信息跨境提供	• 个保法要求的跨境条件：1）通过网信部门的安全评估、2）经专业机构进行个人信息保护认证、3）与接收方签订按照网信部门制定的标准合同或4）法律、行政法规或者国家网信部门规定的其他条件 • 个保法要求境外接收方处理个人信息的活动达到本法规定的个人信息保护标准 • 个保法明确关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在境内收集和产生的个人信息存储在境内 • 个保法要求事前个人信息保护影响评估和取得个人的单独同意
法律责任	• 个保法违法追责更为严厉，包括责令整改（对应用程序责令暂停或者终止提供服务）、没收违法所得、针对组织和人员的罚款、高管禁业、记入信用档案、赔偿损失等

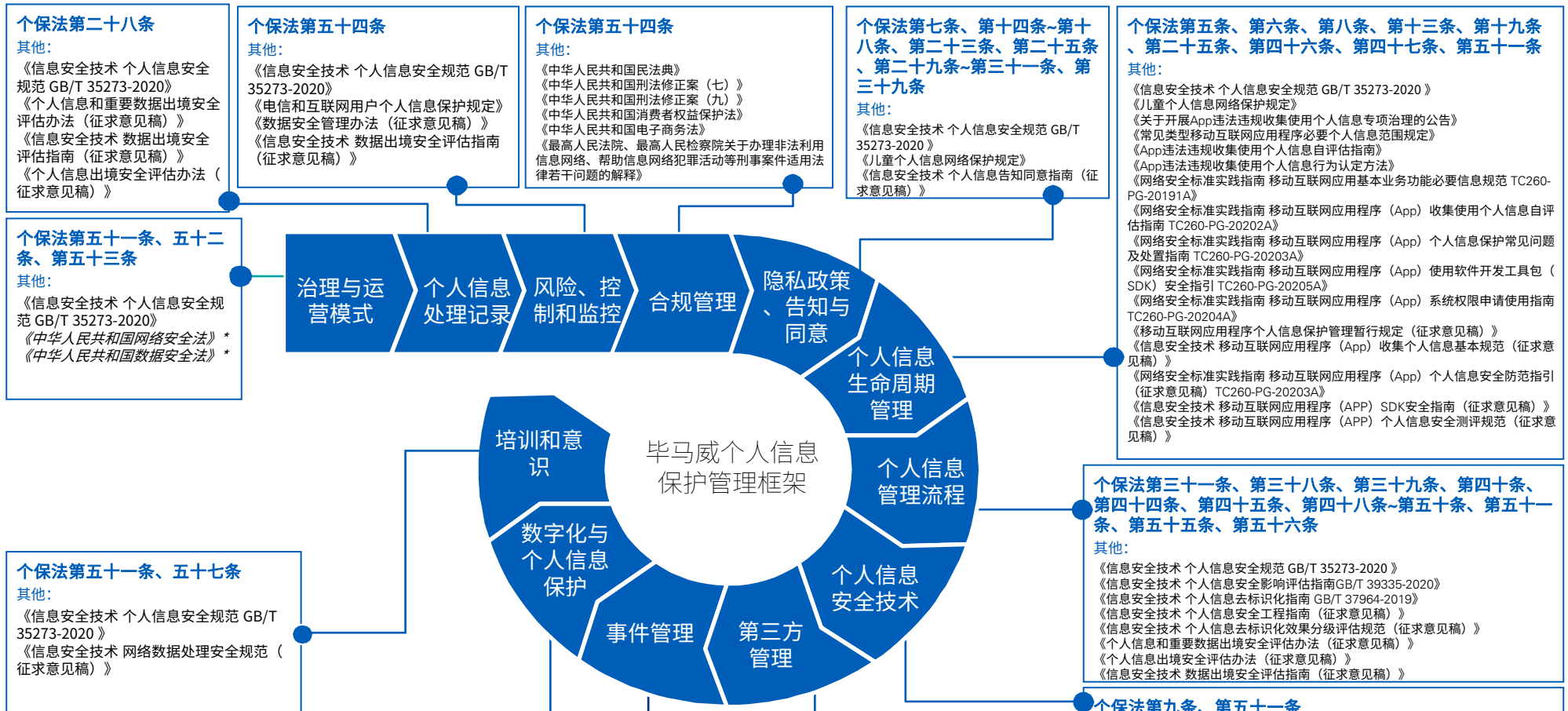
注：EU GDPR指欧盟通用数据保护条例，即 General Data Protection Regulation

关联阅读
学习过GB/T 35273-2020的企业还应关注什么？

适用范围	• -
个人信息处理者	• 个保法下定义“个人信息处理者”和特殊类型的“个人信息处理者”和个人信息安全规范下定义“个人信息控制者” 稍显不同
合法基础	• 个保法处理个人信息取得个人同意的例外情况略有差异，在合理范围内可处理个人自行公开或其他已经合法公开的个人信息，或可处理按照依法制定的劳动规章制度和依法签订法人集体合同实施人力资源管理所必需的个人信息
合规义务	• 个保法要求处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则 • 个保法规定的个人信息主体权利略有差异，尤其是新增了知情权、个人有权要求个人信息处理者对其个人信息处理规则进行解释说明、自然人死亡后主体权利的行使等 • 个保法要求对个人信息进行分类保护 • 个保法要求的个人信息保护影响评估的启动条件和记录保存时长略有差异 • 个保法对APP收集个人信息、“大数据杀熟”、公共场所图像采集等制定了针对性处理规则 • 个保法要求在境内开展分析、评估境内自然人的行为的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表
个人信息跨境提供	• 个保法要求的跨境条件：1）通过网信部门的安全评估、2）经专业机构进行个人信息保护认证、3）与接收方签订按照网信部门制定的标准合同或4）法律、行政法规或者国家网信部门规定的其他条件 • 个保法要求境外接收方处理个人信息的活动达到本法规定的个人信息保护标准 • 个保法明确关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在境内收集和产生的个人信息存储在境内 • 个保法要求事前个人信息保护影响评估
法律责任	• -

注：GB/T 35273-2020 指 信息安全技术 个人信息安全规范

系统化理解个人信息保护合规要求



个保法第二十八条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020》
《个人信息和重要数据出境安全评估办法（征求意见稿）》
《信息安全技术 数据出境安全评估指南（征求意见稿）》
《个人信息出境安全评估办法（征求意见稿）》

个保法第五十四条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020》
《电信和互联网用户个人信息保护规定》
《数据安全管理办法（征求意见稿）》
《信息安全技术 数据出境安全评估指南（征求意见稿）》

个保法第五十四条

其他：

《中华人民共和国民法典》
《中华人民共和国刑法修正案（七）》
《中华人民共和国刑法修正案（九）》
《中华人民共和国消费者权益保护法》
《中华人民共和国电子商务法》
《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》

个保法第七条、第十四条~第十八条、第二十三条、第二十五条、第二十九条~第三十一条、第三十九条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020 》
《儿童个人信息网络保护规定》
《信息安全技术 个人信息告知同意指南（征求意见稿）》

个保法第五条、第六条、第八条、第十三条、第十九条、第二十五条、第四十六条、第四十七条、第五十一条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020 》
《儿童个人信息网络保护规定》
《关于开展App违法违规收集使用个人信息专项治理的公告》
《常见类型移动互联网应用程序必要个人信息范围规定》
《App违法违规收集使用个人信息自评估指南》
《App违法违规收集使用个人信息行为认定方法》
《网络安全标准实践指南 移动互联网应用基本业务功能必要信息规范 TC260-PG-20191A》
《网络安全标准实践指南 移动互联网应用程序（App）收集使用个人信息自评估指南 TC260-PG-20202A》
《网络安全标准实践指南 移动互联网应用程序（App）个人信息保护常见问题及处置指南 TC260-PG-20203A》
《网络安全标准实践指南 移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引 TC260-PG-20205A》
《网络安全标准实践指南 移动互联网应用程序（App）系统权限申请使用指南 TC260-PG-20204A》
《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》
《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范（征求意见稿）》
《网络安全标准实践指南 移动互联网应用程序（App）个人信息安全防范指引（征求意见稿）TC260-PG-20203A》
《信息安全技术 移动互联网应用程序（APP）SDK安全指南（征求意见稿）》
《信息安全技术 移动互联网应用程序（APP）个人信息安全测评规范（征求意见稿）》

个保法第五十一条、五十二条、第五十三条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020》
*《中华人民共和国网络安全法》**
*《中华人民共和国数据安全法》**

个保法第三十一条、第三十八条、第三十九条、第四十条、第四十四条、第四十五条、第四十八条~第五十条、第五十一条、第五十五条、第五十六条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020 》
《信息安全技术 个人信息安全影响评估指南GB/T 39335-2020》
《信息安全技术 个人信息去标识化指南 GB/T 37964-2019》
《信息安全技术 个人信息安全工程指南（征求意见稿）》
《信息安全技术 个人信息去标识化效果分级评估规范（征求意见稿）》
《个人信息和重要数据出境安全评估办法（征求意见稿）》
《个人信息出境安全评估办法（征求意见稿）》
《信息安全技术 数据出境安全评估指南（征求意见稿）》

个保法第五十一条、五十七条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020 》
《信息安全技术 网络数据处理安全规范（征求意见稿）》

个保法第九条、第五十一条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020 》
《关于加强网络信息保护的决定》
《电信和互联网用户个人信息保护规定》
《互联网个人信息安全保护指南》
《信息安全技术 个人信息去标识化指南 GB/T 37964-2019》
《信息安全技术 个人信息去标识化效果分级评估规范（征求意见稿）》
《中华人民共和国网络安全法》
《中华人民共和国数据安全法》
《 信息安全等级保护管理办法 》
《 网络安全等级保护条例（征求意见稿） 》
*网络安全等级保护系列国标

个保法第二十四条、第二十六条、第二十七条、 五十八条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020 》
《禁止网络不正当竞争行为规定（公开征求意见稿）》

个保法第五十一条、第五十七条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020 》

个保法第二十条~第二十二条、第五十九条

其他：

《信息安全技术 个人信息安全规范 GB/T 35273-2020 》

注：建议企业在开展个人信息保护工作时，考虑网安法、数安法的合规要求

履行个人信息保护职责的部门

- **国家网信部门**

  统筹协调个人信息保护工作和相关监督管理工作

- **国务院有关部门**

  依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作

- **县级以上地方人民政府有关部门**

  按照国家有关规定确定个人信息保护和监督管理职责

建立健全个人信息保护管理体系

治理与运营模式
- ❑ 个人信息保护负责人和组织
- ❑ 治理架构与运营模式
- ❑ 制度体系和技术路线规划

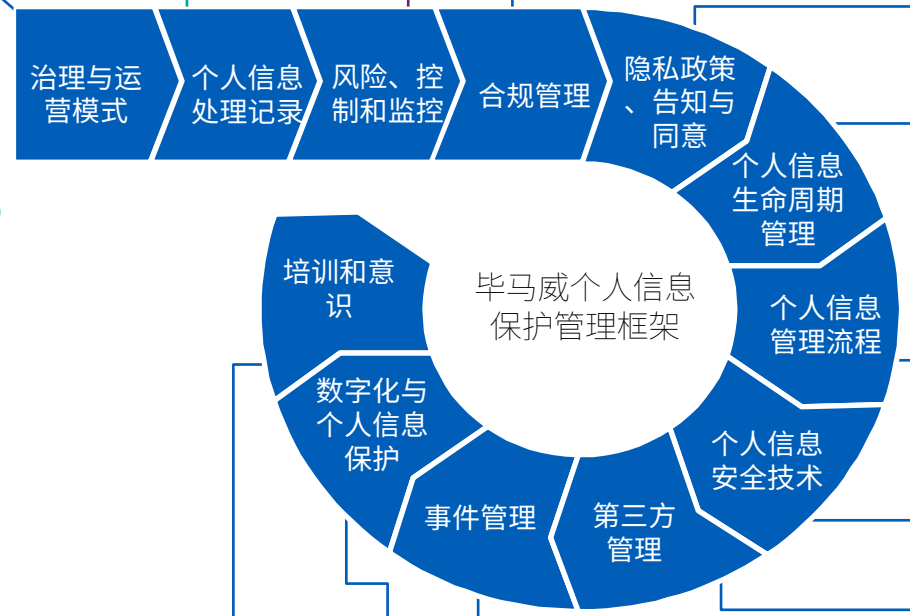
个人信息处理记录
- ❑ 个人信息处理活动记录
- ❑ 数据流图
- ❑ 系统清单

风险、控制和监控
- ❑ 风险和控制
- ❑ 控制检查和监督
- ❑ 合规审计
- ❑ 个人信息保护社会责任监督和报告（如需）

合规管理
- ❑ 合规要求变化跟进
- ❑ 合规要求理解和落实
- ❑ 合规应对和沟通管理

隐私政策、告知与同意
- ❑ 隐私政策
- ❑ 告知与同意
- ❑ 法律文件模板管理

建议的基本工作原则
- ✓ 关注组织和人事保障
- ✓ 基于处理活动和生命周期进行管理
- ✓ 探索技术改进机会



个人信息生命周期管理
- ❑ 合法、正当、必要和诚信原则
- ❑ 个人信息分类分级
- ❑ 个人信息采集（最小化采集）
- ❑ 个人信息质量管理
- ❑ 个人信息共享管理
- ❑ 个人信息保存时限管理
- ❑ 儿童个人信息处理规则

个人信息管理流程
- ❑ 个人信息保护影响评估
- ❑ 个人信息安全工程
- ❑ 个人行使权利的申请受理和处理机制
- ❑ 个人信息跨境传输管理

个人信息安全技术
- ❑ 个人信息操作权限管理
- ❑ 个人信息加密
- ❑ 个人信息去标识化

培训和意识
- ❑ 安全教育和培训

数字化与个人信息保护
- ❑ 自动化决策
- ❑ 处理已公开的个人信息
- ❑ 公共场所收集个人图像、身份识别信息

事件管理
- ❑ 事件应急响应
- ❑ 事件调查取证

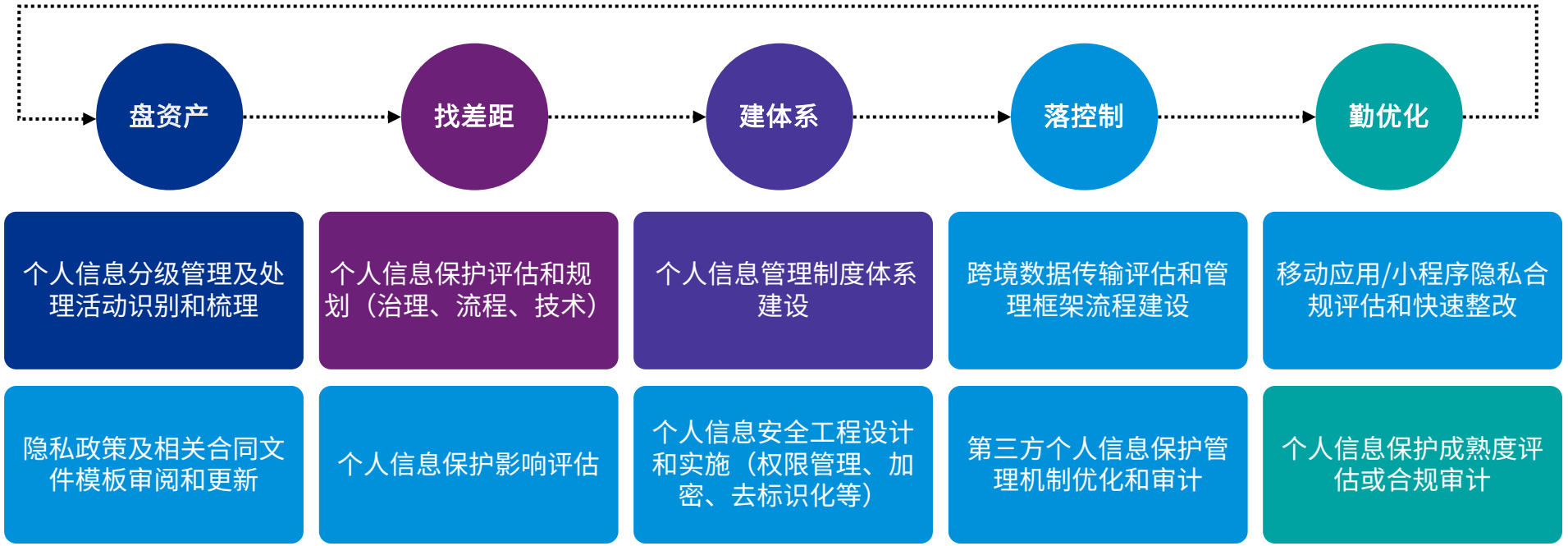
第三方管理
- ❑ 第三方尽职调查
- ❑ 第三方合同模板/数据处理协议
- ❑ 第三方审计管理
- ❑ 特殊场景下的信息转移管理（如合并、分立、解散、被宣告破产等）

优先落实
- ❑ 治理与运营模式
- ❑ 个人信息处理记录
- ❑ 隐私政策、告知与同意
- ❑ 个人信息管理流程
- ❑ 事件管理
- ❑ 培训和意识

重点把控
- ❑ 合规管理
- ❑ 个人信息生命周期管理
- ❑ 个人信息安全技术
- ❑ 第三方管理
- ❑ 数字化与个人信息保护

持续改进
- ❑ 风险、控制和监控

毕马威协助企业解决不同阶段个人信息保护议题



联系我们

石浩然
毕马威中国
网络与信息安全咨询
服务合伙人
电话：+852 2143 8799
henry.shek@kpmg.com

张令琪
毕马威中国
网络与信息安全咨询
服务合伙人
电话： +86 (21) 2212 3637
richard.zhang@kpmg.com

张倪海
毕马威中国
网络与信息安全咨询
总监
电话： +852 2847 5062
brian.cheung@kpmg.com

黄芃芃
毕马威中国
网络与信息安全咨询
总监
电话： +86 (21) 2212 2355
quin.huang@kpmg.com

郝长伟
毕马威中国
网络与信息安全咨询
总监
电话： +86 (10) 8508 5498
danny.hao@kpmg.com