关于推进个人信息保护合规审计的若干建议

个人信息保护合规审计推进小组

2021 年 12 月

编制说明

本报告的编写得到如下单位的支持，在此一并感谢（排名不分先后）

牵头单位

中国信息通信研究院云计算与大数据研究所

指导单位

中国内部审计协会、中国银行业协会、中国通信标准化协会互联网医疗健康标准推进委员会

参与单位

中国移动通信集团有限公司、中信银行、大家保险集团有限责任公司、中移动信息技术有限公司、北京字节跳动科技有限公司、北京三快在线科技有限公司、易车公司、联想集团、贝壳找房（北京）科技有限公司、世辉律师事务所、蚂蚁科技集团股份有限公司、北京小米移动软件有限公司、网商银行等

特别鸣谢专家

沈立强、高峰、何宝宏、刘智伊、张晓瑜、赵成刚、杨玲玲、陈杨、冯天宜、肖竞、梁叶、庞博、李艳东、孟令谦、胡鸣、刘慧博、董才、车蔚玥、周羽杰、雷翔静、岳闻婧、梅亮、常林、李鹏、王雅佳、黄蓉、王新锐、王嘉瑛、刘超域、张向拓、蔚然、马可等

目　录

第一章 引言

当前，全球进入“数据驱动”时代，信息流带动物流、人流、资金流、技术流，创造了巨大价值。但数据爆发增长、海量聚集也带来了日益严峻的安全风险，随意收集、违法获取、过度使用、非法买卖个人信息等乱象频发，引发了广泛关注。为将广大人民群众网络空间合法权益维护好、保障好、发展好，使广大人民群众在数字经济发展中享受更多的获得感、幸福感、安全感，我国先后颁布了《中华人民共和国网络安全法》（简称“网络安全法”）《中华人民共和国民法典》（简称“民法典”）《中华人民共和国数据安全法》（简称“数据安全法”）《中国人民共和国个人信息保护法》（简称“个人信息保护法”）等法律法规，逐步构建起个人信息保护的法治堤坝。

为了建立多层次的个人信息保护合规体系，《个人信息保护法》明确提出了个人信息处理者开展个人信息保护合规审计的要求。第五十四条规定，“个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计”；第六十四条规定，“履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计”。

合规审计是审计机构和审计人员依据国家法律、法规和财经制度对被审计单位的生产经营管理活动及其有关资料是否合规所进行的一种经济监督活动。在个人信息保护合规审计(简称“合规审计”)中,审计机构以独立的第三方视角,依据法律、行政法规等对个人信息处理者的个人信息处理活动进行评价和监督,揭示管理和控制等方面存在的不足,提升个人信息处理者的个人信息保护水平,降低合规风险。

第二章 总体要求

第一节 审计依据

个人信息保护合规审计的审计依据为我国个人信息保护相关现行有效的法律、行政法规。有关部门已发布的法律法规征求意见稿和国家标准亦可作为参考。

建议重点关注的审计依据如下:

一、法律

- 《个人信息保护法》
- 《审计法》
- 《数据安全法》
- 《民法典》
- 《未成年保护法》
- 《电子商务法》
- 《消费者权益保护法》
- 《网络安全法》

二、行政法规

- 《关键信息基础设施安全保护条例》（国令〔2021〕第 745 号）

三、部门规章

- 《儿童个人信息网络保护规定》（国家互联网信息办公室令〔2019〕第 4 号）
- 《电信和互联网用户个人信息保护规定》（工业和信息化部令〔2013〕第 24 号）

四、规范性文件

- 《常见类型移动互联网应用程序必要个人信息范围规定》（国信办秘字〔2021〕14 号）
- 《App 违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191 号）
- 《关于开展 APP 侵害用户权益专项整治工作的通知》（工信部信管函〔2019〕337 号）
- 《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164 号）
- 《关于开展信息通信服务感知提升行动的通知》（工信部信管函〔2021〕292 号）

五、司法解释

- 《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》
- 《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》
- 《关于审理利用信息网络侵害人身权益民事纠纷案

件适用法律若干问题的规定》

六、国家标准

- 《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）

医疗、金融、汽车等不同行业主管监管部门亦会制定相关行业监管规则，企业开展合规审计过程中应对行业监管规则中要求的个人信息保护义务进行核实和遵从。

个人信息保护合规审计依据应随《个人信息保护法》配套规则的完善而不断更新和扩展。

第二节 审计目标

开展个人信息保护合规审计，旨在推动个人信息处理者深入贯彻落实《个人信息保护法》等法律、行政法规要求，健全管理制度、完善技术措施、强化监督管控，助力个人信息保护机制不断完善，规范个人信息处理活动，促进个人信息合理利用，提升组织的个人信息保护水平，切实保障个人合法权益。

第三节 审计原则

开展个人信息保护合规审计，要践行以人民为中心的发展思想，通过依法开展持续、全面、深入的审计工作，及时发现本组织个人信息处理活动中存在的意识不到位、机制不健全、行为不规范等问题，同时要协调好个人信息保护与促

进信息自由流动的关系。在遵循常规审计原则的基础上，个人信息保护合规审计应当着重遵循以下原则：

一、遵循性原则。以法律、行政法规作为依据，判断个人信息处理活动是否合法、合规，同时在审计过程中积极探索，结合审计中发现的新情况，提出切实可行的建议。

二、独立性原则。合理设置组织架构和管理关系，积极营造审计环境，确保审计活动正常进行，不受任何干涉和侵犯。

三、全面性原则。审计范围要覆盖个人信息处理活动全生命周期的各个阶段，审计对象要覆盖数据、信息系统、设备设施、操作人员等多种维度，审计内容要覆盖协议、隐私政策、访问记录、系统日志等，确保审计监督无死角。

四、持续性原则。定期、持续开展个人信息保护合规审计，确保审计监督无空当。加强以信息化手段在具备条件的领域开展常态化、智能化的实时审计。

五、重要性原则。对于敏感个人信息及关键信息基础设施相关的处理活动，要重点关注、全量关注，投入更大力量加强监督。

六、深入性原则。通过多种方式不断提升管理层的重视程度和审计团队的胜任能力，确保审计监督在广度上无盲区、深度上无死角，避免审计工作浮于表面、流于形式。

七、保密性原则。审计工作中所接触的个人信息，必须遵守审计的保密纪律，仅用于审计工作使用，不得随意向外泄露。

第四节 审计人员

执行个人信息保护合规审计工作的审计人员应当遵守中国内部审计协会颁布的《中国内部审计准则》，审计人员在开展审计工作中应当遵循《内部审计人员职业道德规范》的要求，认真履行职责，不得损害国家利益、组织利益和审计职业声誉。

一、审计人员应保持审计工作独立性，遵守职业道德，在实施合规审计业务时保持应有的职业谨慎。审计人员在个人信息保护工作中承担第三方独立监督职责，负责评估被审计对象是否充分建立了个人信息保护机制、所采取的个人信息保护措施是否合理、有效，针对审计中发现的个人信息违规使用、滥用等不合规问题，应及时敦促整改，以确保组织的个人信息处理活动合法、合规。

二、审计人员应具备相应的专业胜任能力，熟悉审计方法论、个人信息保护相关的法律法规要求以及安全技术措施。个人信息保护合规审计团队建议包含掌握信息系统审计、信息系统开发运维、数据安全、信息安全、法律合规等专业知识和技能的专家，以防范审计风险。

三、审计人员应持续接受针对性的培训和宣贯，包括但不限于专业工具的使用，相关法律法规、行业标准和内部组织管理制度的培训等，从而提高审计人员的专业知识和专业技能，保证个人信息保护合规审计工作的顺利实施。

四、个人信息保护合规审计工作实施过程中，审计人员

应对实施审计业务所获取的个人信息保密，非因有效授权、法律规定或其他合法事由不得披露。在社会交往中应当履行保密义务，警惕非故意泄露所获取个人信息的可能性。另外，审计人员不得利用其在实施审计业务时获取的个人信息牟取不正当利益，或者以有悖于法律法规、组织规定及职业道德的方式使用获取的个人信息。

第三章 审计内容

第一节 个人信息处理者义务合规审计

一、概述

个人信息处理者应当根据个人信息的处理目的、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，采取安全保障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。

二、主要风险点

1.【未建立完善的制度体系】未按要求建立个人信息保护合规制度体系。包括个人信息保护内部管理制度和操作规程，以及专门制定未满十四周岁未成年人的个人信息处理细则及个人信息跨境提供细则。

2.【未对个人信息实行分类管理】个人信息处理者内部未结合法律、行政规范要求，自身业务特性、行业要求等制定合理的个人信息分类标准，未全面识别组织涉及的个人信息并进行有效的分类管理。

3.【未采取安全技术措施】未采取网络安全、计算机环境安全、应用和数据安全等基础安全控制措施，未采取加密、去标识化等安全技术措施，未合理分配个人信息处理的操作权限，造成未经授权访问个人信息，以及个人信息泄露、篡改、丢失等。

4.【未定期对从业人员进行安全教育和培训】个人信息处理者未制定个人信息保护安全培训计划，未定期对相关从业人员开展适当的教育和培训。

5.【未制定和实施应急预案】未制定并组织实施个人信息安全事件应急预案，发生个人泄露、篡改、丢失等事件时，未进行及时处置和采取补救措施，未通知履行个人信息保护职责的部门和个人。

6.【未进行个人信息保护影响评估】个人信息处理者在开展对个人权益有重大影响的个人信息处理活动前，未按要求对个人信息处理活动进行事前评估，并对处理情况进行记录及保存。

7.【缺少独立定期监督，未明确平台义务】对于提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，未建立健全的个人信息保护合规制度体系，同时未按照要求使用外部独立机构对组织个人信息保护情况进行监督，未明确平台的个人信息保护规范和义务，未定期发布个人信息保护社会责任报告。

8.【未按要求设置个人信息保护负责人】个人信息处理者未根据自身情况合理制定个人信息保护负责人，负责对

个人信息处理活动以及采取的措施等进行监督，并将个人信息保护负责人的联系方式进行适当的公开和报送。

三、重点审计内容

1.检查个人信息处理者制定的各类内部制度和操作规程，判断其是否在内部管理制度和操作规程针对个人信息保护做了相应的规定，同时评估管理制度制定的合理性和完善性，以及制度和操作规程是否在组织范围内得到有效执行。

2.查阅组织对个人信息分类保护制度的建设情况，评估个人信息分类分级的合理性及全面性，以及是否针对不同类型、级别的个人信息制定了相应的保护策略，同时检查不同类型、级别的个人信息在处理过程中是否得到有效保护。

3.梳理涉及个人信息处理的业务场景、管理流程与信息系统，确认信息系统是否部署了网络安全、通信传输安全等控制措施，在信息系统中启用了身份鉴别控制，对个人信息和敏感个人信息的传输、存储是否采用了合适的加密、去标识化处理。检查信息系统的操作权限表和用户清单、员工岗位清单等，核对个人信息访问权限是否符合“必须知道、最小授权”原则，对于不再需要的访问权限是否及时删除。

4.检查个人信息处理者是否设置了个人信息保护安全培训计划，是否定期对相关从业人员开展教育和培训，培训课时是否未达到相关规定的要求，是否对教育和培训进行记录和留存。

5.检查组织是否制定了个人信息安全事件应急管理预案，并设置了应急管理小组进行定期演练。当出现个人信息

危害事件时，组织是否及时进行调查和处置，是否及时通知个人信息的主体，并保留处理记录。是否部署有效的日志管理机制，以实现对个人信息安全事件进行溯源等。

6. 检查在进行对个人权益有重大影响的个人信息处理活动前是否开展了影响评估，以及评估内容是否合理、全面，并保留相应的影响评估报告至少三年。

7. 针对提供互联网平台服务、用户数量巨大、业务类型复杂的组织，确认是否建立了健全的个人信息保护合规制度体系，是否聘请外部独立机构对其个人信息保护情况进行监督，并检查个人信息保护工作机构设置、信息报送及人员配备和培训管理情况，评估相关组织架构及职责的设计是否能有效推动个人信息保护工作的有序开展。同时，检查组织是否制定了平台规则、明确和约束平台内产品或服务提供者应尽的个人信息保护义务，是否定期发布个人信息保护社会责任报告。

8. 评估个人信息处理者是否达到网信部门要求设置个人信息保护负责人的条件。如达到条件，检查是否设置了个人信息保护负责人，是否明确其岗位职责和权限，汇报路径是否清晰等。以及个人信息保护负责人是否采取了相关措施对个人信息处理活动进行监督。同时，检查个人信息保护负责人的联系方式是否被恰当的公开，是否及时、准确地报送给个人信息保护职责部门。

第二节 个人权利实现方式合规审计

一、概述

明确个人在个人信息处理活动中享有知情权、决定权、查阅复制权、转移权、补充更正权、删除权（被遗忘权）、要求解释权、代行使权等具体权利。同时，个人信息处理者应建立便捷的个人行使权利的申请受理和处理机制，确保个人权利能够有效实现。

二、主要风险点

可能存在不履行响应个人行权义务或设置不合理且非必要的影响个人维权的条件等情形，具体体现为：

1.【未尊重个人的知情权、决定权】未向个人告知必要信息，明示处理的目的、方式和范围，未征得个人的同意。

2.【缺少查阅、复制权实现路径】未能向个人提供查询个人信息、以及获取个人信息副本的路径。

3.【缺少转移权实现路径】未能在特定条件下向个人提供将个人信息转移至其指定的个人信息处理者的途径。

4.【缺少补充、更正权实现路径】未能向个人提供更正或补充信息的路径。

5.【未尊重个人的删除权】无正当理由下未主动删除理应主动删除的个人信息，在个人主张删除时设置不必要或不合理条件。

6.【未尊重个人的要求解释权】未在规定时间内响应个人的要求解释权，或者未达到个人所要求的对个人信息处理规则解释说明的满意程度。

7.【未有效响应个人行使权利的请求】未公布个人行

使权利的申请受理和处理机制，未在规定时间内响应个人的行使各项权利的请求，或行权途径不便捷，设置不必要或不合理条件等。

三、重点审计内容

重点审计是否有效尊重或响应个人的各项权利，审计是否有便捷的个人行使权利的申请受理和处理机制，确保个人权利能够有效实现，具体包括：

1.检查是否通过个人信息处理规则或其他恰当的方式告知个人行使权利的方式和路径。

2.检查组织是否在不同的场景下获得了个人对应程度的同意，如单独同意、重新同意、书面同意等。

3.基于个人同意处理个人信息的，检查个人信息处理者是否提供便捷的撤回同意的方式，并且在个人撤回同意后是否降低服务质量或者直接拒绝提供产品和服务。

4.检查组织是否设置了查阅、复制、更正、删除个人信息或注销用户账号的有效途径，并且没有设置不必要或不合理条件。

5.检查当个人请求将个人信息转移至其指定的个人信息处理者的，若符合国家网信部门规定条件，是否为其提供转移路径。

6.检查当死者近亲属为了自身的合法、正当利益对死者的相关个人信息行使查阅、复制、更正、删除等权利的，是否提供行使权利的方式和路径。

7.检查组织是否设置个人权利申请受理和处理机制以

及时响应个人主体权利请求，是否在对外承诺的时限内响应个人的合理诉求。

第三节 个人信息处理活动合规审计

一、个人信息收集活动合规审计

（一）概述

个人信息处理者在收集个人信息时，首先要遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式主动收集个人信息或者非法买卖方式间接收集个人信息。其次收集应当具有明确、合理的目的，收集的个人信息应当与处理目的直接相关，且应限于实现处理目的最小范围。

（二）主要风险点

1.【未保证收集活动的合法正当性】通过误导、欺诈、胁迫等方式收集其个人信息，通过非法渠道收集个人信息，未通过合同协议等方式明确第三方机构个人信息获取的合法性和个人信息真实性。

2.【个人信息收集缺少合法性基础】收集个人信息的行为不符合法律、行政法规规定，如未取得个人同意、非履行法定职责或法定义务所必需等。

3.【缺少个人信息收集的明确告知】基于个人同意收集个人信息的，未经过明确告知的情况下收集个人信息。如基于隐私政策、告知同意书等个人信息处理规则的告知方式内容不真实、不准确、不完整、不易访问、不清晰易懂，缺少适当的更新和通知等。

4.【未获得个人同意】基于个人同意收集个人信息的，通过各种方式收集个人信息前未获得个人同意，如通过 SDK 代码插件收集、使用手机系统权限（例如相机、麦克风、位置）等。

5.【超范围收集】基于个人同意收集个人信息的，实际收集的个人信息是否超出个人同意的范围。

6.【变更后未重新获得个人同意】基于个人同意收集个人信息的，个人信息的处理目的、处理方式和处理的个人信息种类发生变更后，未重新获取个人同意。

7.【敏感个人信息收集未获得单独同意】针对敏感个人信息的收集，未事前进行个人信息保护影响评估，未获取个人的单独同意。法律、行政法规规定处理敏感个人信息，未获得个人的书面同意。

8.【未向个人告知处理敏感个人信息的必要性以及对个人权益的影响】基于个人同意收集敏感个人信息时，未向个人告知处理敏感个人信息的必要性以及对个人权益的影响。

9.【未成年人信息收集未获得监护人授权同意】针对不满十四周岁未成年人个人信息的收集，未获取未成年人的父母或者其他监护人的同意。

10.【间接收集的个人信息未获得个人同意】针对间接收集的个人信息，未明确个人信息提供方已获得个人的同意，包括使用目的，个人是否同意转让共享等。

11.【未提供同意授权撤回方式或者撤回困难】基于个

人同意收集个人信息的，未提供给个人撤回其同意的功能或者方法，或者为撤回制造不合理操作步骤和障碍。

12.【不同意或撤回同意后停止提供服务或者降低服务质量】个人不同意处理个人信息或者撤回同意后，停止为其提供与其授权个人信息无关的产品或者服务，或者降低其他上述产品或者服务的质量。

13.【收集频率非所必需的最低频率】收集个人信息的频率超出为个人实现产品或服务所必需的最低频率，或者尚未开始为个人提供相应产品或服务时提前收集个人信息。

14.【收集数量非所必需的最小数量】收集的个人信息的数量超出实现产品或服务的业务功能所必需的最少数量。

（三）重点审计内容

重点审计组织内的个人信息收集过程时的合法性和正当性、明确告知、经过授权同意，以及符合最小必要原则。

1.梳理所有自主收集个人信息的业务场景，评估其是否存在充分合理的合法依据。评估收集过程中是否可能存在欺诈、误导、胁迫个人的情况。梳理所有间接收集个人信息的业务场景，评估其是否存在充分合理的合法依据。针对基于合同协议方式获取个人信息的情况，审阅并评估第三方机构的背景资质、以及个人信息的合法性和真实性。

2.梳理所有收集个人信息的业务场景，评估个人信息收集是否基于个人同意，如非基于个人同意，评估是否基于《个人信息保护法》以及其他法律、行政法规规定的可处理个人信息的情况。

3.审阅告知个人的过程中，是否告知其收集的个人信息明细、处理目的、方式和范围等。审阅隐私政策、告知同意书等个人信息处理规则是否以显著方式公开，语言是否清晰易懂，内容是否真实、准确、完整地涵盖个人信息处理者的名称或者姓名和联系方式；个人信息的处理目的、处理方式、处理的个人信息种类、保存期限；个人行使本法规定权利的方式和程序。审阅个人信息处理规则的更新流程，检查是否及时将变更内容告知于个人。

4.梳理并审阅个人信息收集流程和相关系统功能设计：

（1）基于个人同意收集个人信息的，确认只有经过个人同意后才开始个人信息收集动作（包括自动收集的个人信息）。

（2）针对敏感个人信息的收集，确认已经获取个人的单独同意；如果按照法律和行政法规规定应当获取书面同意的情况，确认是否获取书面授权同意。

（3）确认是否针对不满十四周岁未成年个人信息进行单独管理，包括：不满十四周岁未成年人进行区分标识，以及个人信息的收集需获取未成年人的父母或者其他监护人的同意。

（4）分析比较个人同意的时间点和个人信息收集的时间点，确认是否存在未获得同意的情况下进行了个人信息收集的情况。

5.对比个人同意收集的实际收集的个人信息类型、范围和频率等的差异，评估是否超范围收集个人信息。

6.审阅个人信息同意更新流程，确认是否已经建立流程确保个人信息处理目的、处理方式或处理的个人信息种类发生变更后，可以及时获取个人的再次授权同意。

7.检查收集敏感个人信息时，是否通过隐私政策、告知同意书等个人信息处理规则向个人告知处理敏感个人信息的必要性以及对个人权益的影响，评估告知是否显著、清晰，并且已获取个人的充分理解。

8.针对间接收集的个人信息，确认是否存在适当流程支持：

（1）确保第三方机构（即个人信息提供方）或组织自身已获得个人的同意，包括使用目的、个人是否同意转让共享等。

（2）针对开展业务所需进行的个人信息处理活动超出已获得的同意范围的情况，能够及时获取个人的明示同意，或通过个人信息提供方征得个人的明示同意。

（3）审阅间接收集的个人信息，确认其处理目的在授权范围内。

9.确认是否为个人提供同意授权的撤回功能和方法。审阅撤回功能的设计确认是否存在不合理操作步骤或者前置条件。

10.针对个人拒绝授权或者撤回授权同意后，确认是否存在继续收集其个人信息，或频繁打扰尝试获取授权，降低服务质量，拒绝提供非必要个人信息时是否会拒绝其提供基础功能服务等不合规情况。

11.排查产品或服务在上线前是否收集敏感个人信息，如收集敏感个人信息是否经过个人信息保护影响评估，评估内容是否涵盖最小必要原则。

12.针对收集的个人信息，确认收集的频率是否是实现产品或服务的业务功能所必需的最低频率。

13.针对收集的个人信息，确认收集的数量是实现产品或服务的业务功能所必需的最少数量。

二、个人信息存储活动合规审计

(一)概述

个人信息处理者对信息的保存期限应当为实现处理目的所必要的最短时间，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，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。个人信息处理者应当采取控制措施确保个人信息存储活动符合法律、行政法规的规定，并保障个人信息存储的安全性。

（二）主要风险点

1.【保存期限设定过长】组织未按照实现处理目的所必要的最短时间定义保存期限。

2.【未将收集和产生的个人信息在境内存储】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未将在我国境内收集和产生的个人信息在境内存储。

3.【未加密和去标识化处理】组织在存储个人信息时

未采取加密和去标识化等安全技术措施，导致个人信息被泄露或篡改。

4.【缺乏备份和恢复策略】未对个人信息实施有效的备份和恢复策略。一旦发生安全事件或重大灾害，无法及时对重要数据进行恢复，数据完整性和可用性得不到保证。

（三）重点审计内容

1.审阅组织内个人信息的存储期限政策，确定其是否符合相关要求，包括存储期限是否定义在为实现处理目的所需的最短时间范围内。梳理组织范围内存储的个人信息，确定这些信息都在存储期限内。

2.评估是否为关键信息基础设施运营者或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，如是，则梳理组织范围内存储的个人信息，确定这些信息是否存储在境内。

3.梳理组织内存储的个人信息，审阅并确认其按照个人信息的分类分级结果，针对不同等级的个人信息采用不同的存储方式。审阅并确认其分类分级高于一定级别的个人信息经过数据加密和去标识化管理，加密算法应符合安全策略要求，将去标识化后的数据与可用于恢复识别个人的信息分开存储，并确保在后续的个人信息处理中不重新识别个人。存储个人生物识别信息时，是否采用技术措施处理后再进行存储，例如仅存储个人生物识别信息的摘要。

4.审阅组织是否未对个人信息存储设置了有效的备份和恢复策略，是否建立了本地/异地灾备系统，或者采取了其

他必要的措施保障所存储的个人信息的安全。

三、个人信息使用、加工活动合规审计

（一）概述

个人信息处理者应当在个人信息的展示、委托处理、加工处理等操作过程中进行保护，确保个人信息的使用符合法律、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。

（二）主要风险点

1.【个人信息超约定范围使用并未重新征得同意】使用个人信息时超出与收集个人信息时所声称的具有直接或合理关联的范围；因业务需要，确需超出上述范围使用个人信息的，未重新征得个人明示同意。

2.【未能遵守自动化决策方式相关规定】通过自动化决策方式使用个人信息时，未事前进行个人信息保护影响评估，未能保证决策的透明度和结果的公平、公正，对个人在交易价格等交易条件上实行了不合理的差别待遇；未能提供不针对个人特征的选项或向个人提供便捷的拒绝方式；未能满足个人提出的解释或拒绝请求。

3.【未对个人敏感信息脱敏展示】未采取信息屏蔽或截词等处理措施，导致个人敏感信息在展示过程中泄露或被未经授权的拷贝。

4.【未对个人信息查询进行授权管理】未严格限制批量查询，未对个人信息的查询、编辑、导出等操作进行权限

控制，未对敏感信息查询进行授权管理和行为审计。

5.【未对涉及个人信息的委托处理行为进行规范】委托行为超出已征得个人授权同意的范围；未对委托行为进行个人信息保护影响评估；未对受托人进行评估和安全检查；未通过合同等方式规定受托人的责任和义务；未准确记录和保存委托情况；未对受托人的个人信息处理活动进行监督。

6.【未对个人信息加工处理过程进行防泄漏管控】未建立个人信息使用过程中的防泄露控制规范和机制；未防止个人信息使用过程中的调试信息、日志记录等因不受控制的输出而泄露。

7.【缺乏对个人信息汇聚融合的规范】个人信息汇聚融合的技术超出收集时所声明的使用范围；个人信息汇聚融合对个人权益有重大影响，未开展个人信息保护影响评估；未采取有效的技术保护措施。

8.【未对开发测试环境中个人信息的使用进行规范】开发测试环境与生产环境未实现有效隔离；开发、测试环境中未对个人敏感信息进行脱敏处理。

9.【未合理使用已合法公开的个人信息】未在合理范围内使用已合法公开的个人信息。

10.【未合理使用在公共场所收集的个人信息】在未取得个人单独同意的前提下，将在公共场所收集的个人图像、身份识别信息用于维护公共安全之外的目的。

（三）重点审计内容

1.检查使用个人信息时，是否超出与收集个人信息时所声称的具有直接或合理关联的范围；因业务需要，确需超出上述范围使用个人信息的，是否再次征得个人明示同意。

2.审阅组织是否有梳理利用个人信息进行自动化决策的场景，并针对每个场景都提供了不针对个人特征的选项或便捷的拒绝方式；检查组织是否披露了使用自动化决策的方式对个人权益所产生的影响；检查组织是否利用个人信息特征进行了差异化定价。

3.访谈被授权访问个人信息的人员，调阅相关制度和文件，穿行测试信息系统，检查相关系统的个人信息展示时是否对敏感字段进行屏蔽处理；是否对个人信息进行展示过程中具有防止被未经授权的拷贝功能。

4.判断是否相关系统对个人信息的明文展示或者批量下载操作记录了详细的日志并且定期对其日志进行审计；是否建立最小授权的访问控制策略；个人敏感信息的查询、下载和打印是否都取得了相关的审批并且具有真实的业务背景。

5.调阅相关合同、履职等文档，走访第三方机构分析其业务逻辑，对第三方信息系统进行穿行测试，判断将收集的个人信息委托给第三方机构处理时，委托行为是否超出已征得个人授权同意的范围；是否对委托行为进行个人信息保护影响评估，确保受托人具备足够的数据安全能力，且提供了足够的安全保护措施；是否对受委托者进行

安全检查和评估；是否通过合同等方式规定受委托人的责任和义务；是否准确记录和保存委托处理个人信息的情况；是否对受托人的个人信息处理活动进行监督；检查委托合同不生效、无效、被撤销或者终止时，受托人是否返还了个人信息或进行了删除。

6. 检查去标识化处理的数据集或其他数据集汇聚后是否能够重新识别出个人；检查是否建立了个人信息使用过程中的防泄露控制规范和机制。

7. 调阅个人信息脱敏规则，判断是否存在相同信息脱敏规则不一致，导致个人信息通过汇聚融合后获得完整信息。

8. 调阅网络拓扑图，判断开发测试环境与生产环境是否实现隔离；穿行测试信息系统，判断开发和测试环境使用的个人敏感信息是否进行了脱敏处理；抽查历史数据，判断跨网传输是否涉及个人敏感信息、是否经过相应的授权审批、是否及时清除。

9. 检查组织是否将自身收集的个人信息和个人自行公开或者其他已经合法公开的个人信息进行区别，并明确了相应的使用规则。检查在公共场所收集的个人图像、身份识别信息是否只用于维护公共安全的目的，如若用于其他目的是否取得了个人的单独同意；检查对于已合法公开的个人信息的使用是否在合理范围内。

四、个人信息提供活动合规审计

（一）概述

个人信息原则上不得共享和转让，如果确需共享与转让时，必须遵循告知原则、征得个人同意、且需提前进行个人信息保护影响评估。

（二）主要风险点

1.【未尽到告知义务的个人信息提供】对外提供个人信息前未能向个人说明具体场景、个人信息类型、目的、期限、处理方式、双方权利义务、第三方名称及联系方式等并获取个人同意。

2.【超范围提供】个人信息提供超出个人同意范畴。

3.【个人信息保护影响评估缺失】个人信息提供前或场景发生变化后未及时进行个人信息保护影响评估，或者个人信息保护影响评估记录保存不达要求。

4.【未对接收方进行约束限制】未和接收方签署个人信息保护责任承诺；未和接收方明确了提供的约定场景、个人信息类型、目的、期限、处理方式、双方权利义务、第三方名称及联系方式；未准确记录并保存提供的实际情况。

（三）重点审计内容

1.检查组织是否向个人告知个人信息提供的场景、方式、实现等并获取同意。

2.检查个人信息提供存在哪些场景，是否超出了授权同意的范畴。

3.检查个人信息提供场景发生变化是否进行了个人信息保护影响评估，评估记录是否详细准确保存。

4.检查是否和接收方签署了责任协议，明确了提供的约定场景、个人信息类型、目的、期限、处理方式、双方权利义务、第三方名称及联系方式等。检查是否对提供行为和实际情况进行了准确记录和保存。

五、个人信息传输活动合规审计

（一）概述

个人信息在传输环节，应采取管理手段与技术手段，确保个人信息在传输过程中的完整性、保密性、真实性，重点关注个人信息在传输的过程中的篡改、伪造、窃取等安全风险，以及传输行为是否获得适当的授权。

（二）主要风险点

1.【未对个人信息传输进行分级管控】在传输个人信息时，未根据个人信息分级分类原则对个人信息传输进行分级管控，导致个人信息在传输过程中造成泄露。

2.【未经授权和批准进行传输】在传输个人信息前，未获得相应的授权和审批。

3.【未对个人信息进行校验】未对个人信息进行校验，个人信息在传输过程中可能被恶意篡改。

4.【未采取有效措施保障传输安全】未采用防火墙、入侵检测等安全技术，导致传输网络的安全性存在隐患。

（三）重点审计内容

1.确认个人信息处理者在传输个人信息时，是否根据个人信息分级分类原则对个人信息传输进行分级管控。

2.确认个人信息处理者在个人信息传输过程中，是否获得相应的授权和审批。

3.确认个人信息处理者在传输环节，是否采取管理与技术手段，确保个人信息传输过程中的完整性、保密性和真实性。

4.确认个人信息处理者是否采用防火墙、入侵检测等安全技术，确保传输网络的安全性。

六、个人信息公开活动合规审计

（一）概述

个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。个人信息处理者公开个人信息前应当进行个人信息保护影响评估，并针对公开披露渠道建立适当的保护措施，以及对公开披露的过程进行适当的记录。

（二） 主要风险点

1.【未经过单独同意进行公开披露】未经过个人的单独同意，向社会或不特定人群发布其个人信息。

2.【公开披露前未进行个人信息保护影响评估】在进行公开披露前，未开展个人信息保护影响评估，评估公开的法律授权问题、安全控制问题及造成的风险和影响。

3.【公开披露缺少适当信息保护措施】公开披露渠道缺少适当的信息保护措施，导致披露的个人信息被篡改。

4.【公开披露情况缺少准确记录】未准确记录和保存个人信息的公开披露情况，包括：公开披露的合法依据、公开披露的个人信息明细、公开披露的日期、规模、目的、渠道、范围等。

5.【个人信息处理规则缺少公开披露的规则】组织存在个人信息公开披露的情况，但是个人信息处理规则中未明确公开披露的规则，公开披露的目的、涉及的个人信息类型等信息。

（三）重点审计内容

1.审阅组织所有对外公开的个人信息处理规则，确认其已经涵盖公开披露的规则。

2.审阅组织在公开披露个人信息前进行了个人信息安全影响评估，并对个人信息保护影响评估过程和结果进行了详细记录。

3.梳理确认组织的所有针对任何个人信息的公开披露，并审阅历史公开披露相关记录，包括但不限于：每次个人信息公开披露的合法依据、公开披露的个人信息明细、公开披露的时间、披露渠道等。然后进行后续验证确认公开披露过程的合规性。另外，单独审阅公开披露渠道的信息安全保护措施，以确认其有效性。

七、个人信息删除活动合规审计

（一）概述

个人信息处理者应该对符合删除条件的个人信息进行

主动删除，删除条件包括但不限于处理目的已实现、无法实现或者为实现处理目的不再必要、服务停止或者保存期限已届满、个人撤回同意、个人信息处理者违反法律、行政法规或者违反约定处理个人信息。个人信息处理者未删除的，个人有权请求删除。

（二）主要风险点

1.【未主动删除信息】在满足法律法规规定的情形下，组织未主动对相关个人信息进行及时删除。

2.【缺乏受理个人删除需求的途径】组织未建立接收个人信息删除需求的途径，导致个人无法向组织发出删除个人数据申请。

3.【未能按照个人要求删除个人信息】组织无法按照个人需求对组织内所有相关个人信息进行识别和删除。技术上难以实现删除的，未对个人进行解释说明。

（三）重点审计内容

1.审阅个人信息处理者对信息删除的相关规定，确定该规定涵盖了组织应删除个人信息的场景和条件，以及执行删除的必要步骤。梳理个人信息处理者存储的个人信息，确保根据法律法规要求，主动执行了个人信息数据删除。

2.审查个人信息处理者对个人需求受理渠道，确保组织开通了受理个人信息删除需求的受理渠道和相关处理流程。

3.基于组织受理的个人信息删除需求，审阅组织所有存储个人信息的系统确保相关个人信息被及时删除。技术上

难以进行删除的，检查组织是否采取了除存储和必要的安全保护措施以外的处理，并且向个人进行了解释说明，解释说明的沟通记录是否进行了留档。

第四节 个人信息跨境提供合规审计

一、概述

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在中华人民共和国境内运营中收集和产生的个人信息原则上应存储在中国境内，确因为业务需要向境外提供的，个人信息处理者应当按照国家网信部门会同国务院有关部门制定的办法和相关标准进行安全评估，并符合其要求。

二、主要风险点

1.【不满足条件的跨境提供】不满足下列条件之一的个人信息跨境提供：

（1）未通过国家网信部门安全评估的个人信息跨境提供。

（2）缺少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的个人信息跨境提供。

（3）缺少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的个人信息跨境提供。

（4）其他不能满足法律、行政法规、国家网信部门规定的其他条件或者中华人民共和国缔结或者参加的国际条

约、协定相关规定的个人信息跨境提供。

2.【个人信息保护影响评估缺失】个人信息跨境提供前未进行个人信息保护影响评估。

3.【未尽到告知义务并获取同意】个人信息跨境提供前未能告知境外接收方的名称或姓名、联系方式、处理目的、方式、个人信息的种类等，并获取个人的单独同意。

4.【未经批准向外国司法或者执法机构提供信息】未经批准向外国司法或者执法机构提供中华人民共和国境内的个人信息。

5.【向禁止提供名单中的组织或个人提供个人信息】个人信息处理者向国家网信部门列入限制或者禁止个人信息提供清单的组织和个人提供个人信息。

6.【安全保障措施缺失】未能对跨境提供的数据提供有效的安全保障。

三、重点审计内容

1.检查个人信息出境是否满足法律法规对个人信息跨境提供的前提条件。

2.检查个人信息跨境提供前是够进行了个人信息保护影响评估。

3.检查个人数据跨境提供前是否尽到告知义务，并获取了个人的单独同意。

4.检查组织是否存在向外国司法或者执法机构提供中华人民共和国境内的个人信息的情形，若有，是否经过批准。

5.检查组织是否向国家网信部门列入限制或者禁止个

人信息提供清单的组织和个人提供个人信息。

6. 检查是否在个人信息跨境提供中采取了有效措施保障个人信息安全。

第四章 审计程序

合理科学地设计和实施审计程序，其目的是确保收集到充分适当的审计证据以对审计事项进行审查和评价，从而实现审计目标。审计程序应全面关注组织风险及可能导致的审计风险。完整的审计程序包括计划、准备、实施、报告及后续追踪等多个阶段，本文仅针对个人信息保护合规审计特殊性选取了以下重要程序进行描述：

一、审计计划

个人信息保护合规审计应纳入组织总体审计规划范围。组织应充分考虑个人信息保护法律法规要求，根据实际业务情况、个人信息使用场景、个人信息处理活动和保护措施、以及内部技术能力等，评估个人信息保护合规风险，确定个人信息合规审计工作方向、范围、内容、方式、频次以及实现全覆盖的步骤与周期等。审计规划应定期根据法律法规政策变化和发展趋势、同业机构因违规违法处罚事项、内部管理需求和发生的风险或违规事件、以及个人信息保护内控机制和流程变化等因素动态调整滚动更新。

年度审计计划应基于审计规划结果，结合审计资源、审计专业能力、审计工具等合理安排适当的个人信息保护合规

审计，包括专项审计、持续审计或在其他审计项目中同步开展个人信息保护合规审计相关内容等。随着审计规划的动态变化，审计计划应定期进行调整，确保审计及时关注组织在个人信息保护方面的合规风险。

二、审计方案

1.制定审计方案前，应对组织的个人信息处理活动范围、现有个人信息保护建设及执行情况完成初步了解。

2.用以决定审计范围的风险评估应充分考虑：各业务场景涉及的个人信息数量级、个人信息种类、个人信息泄露投诉、已识别的个人信息安全事件、新上线的系统、与个人信息处理相关的新业务流程、涉及个人处理的人员、外部监管压力等。

3.制定审计方案时应考虑开展审计所需的审计人员的能力，包括审计人员对个人信息处理的业务流程、信息系统和法律法规要求等方面的熟悉和了解程度。如果内审团队无法满足所需能力，需要考虑联合组织内部其他负责个人信息管理的部门或者外部专业机构组成联合项目组共同开展，同时保证不对审计的独立性产生损害。

4.制定审计方案时应充分考虑个人信息保护相关的法规法规、部门规章制度、国家标准、行业规范、地方法规和落地最佳实践。

5.如果审计结果会依赖外部专家或者外部审计的工作

结果，审计方案中需要明确对外部工作结果的验证流程以及利用范围。

6.审计方案需要与组织内部负责个人信息管理的相关负责人进行充分沟通，确保审计范围的完整性和适当性。

7.如果审计方案中包含渗透测试等特殊技术方法，需提前做好预案，并与相关团队完成沟通。

三、审计通知

审计机构应当在审计实施前向被审计单位发出审计通知书，审计通知书应包括以下基本内容：被审计机构及审计项目名称；审计目的及审计范围；审计开始时间；审计小组成员；审计所需资料清单等。

鉴于个人信息保护合规审计的特殊性，审计通知对象中应包含组织内部负责个人信息保护的负责人或者相关团队，另外也可采用小范围通知或进场同步通知的突击审计程序。

四、审计实施

1.审计机构进驻被审计单位后，一般应当与被审计单位举行进场会谈。进场会谈的内容包括介绍审计机构成员及分工，说明审计目的、审计范围，听取被审计单位介绍基本情况，提出配合审计的要求。

2.现场审计时，审计人员对相关人员进行谈话，对信息系统中个人信息的处理、保护措施设计和实施情况进行了解。

3.审计人员通过对管理制度、安全策略和机制、合同协议、安全配置和设计文档、运行记录等进行观察、查验、分析，以便理解、分析。

4.审计人员检查处理个人信息的信息系统所处网络环境、处理个人信息的信息系统与其他系统的交互方式。

5.通过人工或自动化安全测试工具进行技术测试，获取相关信息，并进行分析取证。

6.审计执行中应当注意数据来源的可靠性，原则上应当查看、获取、处理及分析原始数据，原始数据不适宜进行上述操作的，应当采取可靠措施确保用于审计的备份数据与原始数据一致。

7.审计人员应根据风险评估结果实施不同类型的审计程序，如在内部控制有效的环节实施控制测试，在内部控制薄弱或者风险水平高的环节实施实质性测试。

8.审计人员在审计过程中应确保对接触到的个人信息进行充分的保护，并对所有涉及到个人信息的操作进行操作日志记录。

五、沟通和报告

审计发现问题后，审计机构应当与被审计单位进行充分的沟通和确认。现场审计结束后，审计机构应当根据沟通内容的要求，选择会议形式或面谈形式与被审计单位及其相关人员进行沟通，应当注意沟通技巧，进行平等、诚恳、恰当、

充分的交流。

审计报告初步完成，并经有权机构审议通过后，由审计机构征求被审计单位意见。如果被审计单位在规定时间内反馈意见，审计机构应结合反馈意见的合理性和必要性对报告进行修改和完善，然后正式呈文。鉴于合规审计的特殊性，审计机构在个人信息保护合规审计报告沟通阶段除了与业务部门沟通之外，还需要与组织内部的法务、安全、合规、大数据、办公室、舆情、人力资源、信息技术等相关部门进行充分沟通，确认是否符合当前实践。审计报告主要包括下列内容：

（一）审计概况：对个人信息保护合规审计项目总体情况的介绍和说明。

（二）审计依据：实施个人信息保护合规审计所依据的相关法律、行政法规、政策文件、国家标准等。

（三）审计结论：根据已查明的事实，对被审计单位涉及个人信息处理的业务、运营、管理等活动，以及内部控制和风险管理的合规性、适当性和有效性作出的评价。

（四）审计发现：对被审计单位涉及个人信息处理的业务、运营、管理等活动，以及内部控制和风险管理实施审计过程中所发现的主要合规问题的事实、定性、原因、后果或影响等。

（五）审计意见：针对审计发现的被审计单位在涉及个人信息处理的业务、运营、管理等活动，以及内部控制和风险管理等方面存在的违反法律、行政法规的情况，提出审计

处理意见；或者建议组织管理层和相关部门做出处理意见。

（六）审计建议：针对审计中发现的被审计单位涉及个人信息处理的业务、运营、管理等活动，以及内部控制和风险管理等方面存在的主要问题，以及其他需要进一步完善提高的事项，在分析原因和影响的基础上，提出有价值的建议。

审计人员在运用专业判断，综合分析收集到的相关证据，撰写审计报告、形成审计结论的过程中需要注意下列事项：

（一）围绕审计目标，依照相关法律法规、政策、程序及其他标准，对审计事项进行评价，评价应当客观公正，并与审计发现问题有密切的相关性。

（二）审计评价应当坚持全面性和重要性相结合，定性与定量相结合的原则。

（三）只对已审计的事项发表审计评价意见，对未经审计的事项、审计证据不充分、评价依据或者标准不明确以及超越审计职责范围的事项，不发表审计评价意见。