TC260-PG-2023XX

网络安全标准实践指南

—粤港澳大湾区跨境个人信息保护要求

（征求意见稿 v1.0-202311）

全国信息安全标准化技术委员会秘书处

2023 年 11 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

本《实践指南》版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、中国网络安全审查技术与认证中心等单位的技术支持。

摘　要

为促进粤港澳大湾区个人信息跨境安全有序流动，推动粤港澳大湾区高质量发展，依据《关于促进粤港澳大湾区数据跨境流动的合作备忘录》（以下简称“备忘录”）和属地相关法律法规，制定本文件。

本文件规定了粤港澳大湾区跨境处理个人信息应遵循的基本原则和保护要求，为实施粤港澳大湾区个人信息保护认证提供了认证依据，也为大湾区个人信息处理者规范个人信息跨境处理活动提供参考。

目 录

1 范围

本文件规定了粤港澳大湾区跨境处理个人信息应遵守的基本原则和要求。

本文件适用于大湾区内个人信息处理者依据备忘录以认证方式开展个人信息跨境处理活动。大湾区内个人信息处理者是指注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内的个人信息处理者，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，及香港特别行政区的个人信息处理者。

2 术语定义

2.1 个人信息

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。

注：个人信息处理者处理的个人信息，按照属地个人信息保护法律确定。例如：内地个人信息处理者处理的个人信息，按照《中华人民共和国个人信息保护法》确定；香港处理的个人信息，按照香港《个人资料（私隐）条例》的“个人资料”确定。

2.2 个人信息主体

个人信息所标识或者关联的自然人。

注：香港也称为“资料当事人”，即就个人资料而言，属该资料的当事人的个人。

2.3 个人信息处理者

个人信息处理者是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

注：香港也称为“资料使用者”，即就个人资料而言，指独立或联同其他人或与其他人共同控制该资料的收集、持有、处理或使用的人。

2.4 个人信息处理

包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等处理活动。

注：就香港而言，涵盖个人信息的收集、持有、处理或使用(包括披露或移转)。其中，“存储”与香港的“持有”对应，“使用、加工”与香港的“处理”对应，“提供、公开”与香港的“使用”对应。

2.5 属地法律法规

就内地而言，是指《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规。就香港特别行政区而言，是指《个人资料（私隐）条例》等法律法规。

3 基本原则

3.1 合法、正当、诚信原则

个人信息处理者在跨境处理个人信息时，应遵循合法、正当、诚信原则，主要包括:

a）遵守属地法律法规等要求;

b）不得通过误导、欺诈、胁迫等方式处理个人信息;

c）处理个人信息应具有明确、合理的目的;

d）跨境处理个人信息应遵守合同、协议等具有法律约束力文件的约定和承诺，不得违背约定和承诺损害个人信息主体的合法权益。

3.2 最小必要原则

跨境处理个人信息应当与处理目的直接相关，限于实现处理目的的最小范围，采取对个人权益影响最小且公平的方式。

3.3 公开透明原则

个人信息处理者在跨境处理个人信息时，应当遵循公开、透明原则，公开个人信息处理规则，明示个人信息处理的目的、方式和范围。

注：公开个人信息处理规则，通常采用隐私政策等方式公开。

3.4 质量保障原则

个人信息处理者在跨境处理个人信息时应保障个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

3.5 确保安全原则

个人信息处理者应当采取必要措施保障跨境处理个人信息的安全和保密，防止未经授权的访问以及个人信息泄露、篡改、丢失、滥用。

3.6 责任明确原则

个人信息处理者应当对其个人信息跨境处理活动负责，保障个人信息主体权益，对损害个人信息合法权益的行为承担责任。

4 个人信息处理要求

4.1 个人信息处理合法性基础

个人信息处理者处理个人信息应符合属地法律法规要求，具体包括:

a）就内地的个人信息处理者而言，处理个人信息应当符合下列情形之一:

1) 取得个人的同意;

2) 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;

3) 为履行法定职责或者法定义务所必需;

4) 为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需;

5) 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息;

6) 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;

7) 法律、行政法规规定的其他情形。

b）就香港的个人信息处理者而言，处理个人信息应符合香港《个人资料(私隐)条例》相关规定（包括其附表一的保障资料原则）。

4.2 个人信息告知同意

个人信息处理者收集个人信息，应符合以下要求:

a）收集个人信息之时或之前，应向个人信息主体告知个人信息收集目的、方式、范围，以及是否可选收集、向哪些类型接收方提供个人信息，属地法律法规另有规定的除外;

b）制定并公开个人信息处理规则，以显著方式、清晰易懂的语言真实、准确、完整明示下列事项:

- 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;
- 对外提供的个人信息种类、目的和接收方;
- 个人信息主体权利、行使方式和程序。

c）基于个人同意处理个人信息的，该同意应由个人信息主体在充分知情的前提下自愿、明确作出;

d）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的，应重新取得个人信息主体同意;

e）处理未成年人个人信息的，应当按照属地法律法规要求取得未成年人的父母或者其他监护人的同意，属地法律法规另有规定的除外。

注：就内地而言，处理不满14周岁未成年个人信息的，应当取得未成年人的父母或者其他监护人同意；就香港而言，收集不满18周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的订明同意。

f）只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，方可跨境处理生物识别、宗教信仰、特定身份、金融账户、医疗健康、行踪轨迹等敏感的信息;

g）不应以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，处理个人信息属于提供产品或服务必需的除外。

4.3 个人信息存储、使用、加工

个人信息处理者存储、使用、加工个人信息，应符合以下要求:

a）除属地法律法规另有规定外，个人信息的保存期限应为实现处理目的所必要的最短时间;

b）个人信息存储期限届满后，应对个人信息进行删除或匿名化处理;

c）如法律法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，应停止除存储和采取必要的安全保护措施之外的处理;

d）使用个人信息进行商业营销，应向个人信息主体告知处理目的、处理方式和处理的个人信息种类，并征得个人信息主体同意;

e）使用个人信息进行商业营销，应向个人提供便捷的拒绝方式，个人信息主体可随时要求处理者停止在商业营销中使用其个人信息;

f）通过自动化决策方式作出对个人权益有重大影响的决定，个人有权按属地法律法规行使个人权利，如要求个人信息处理者予以说明，拒绝个人信息处理者仅通过自动化决策的方式作出决定;

注：自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

g）两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应约定各自的权利和义务。

4.4 个人信息委托处理、提供、公开

个人信息处理者委托处理、提供、公开个人信息，应符合以下要求:

a）委托处理个人信息的，应与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督;

b）受托人应按照约定处理个人信息，不应超出约定的处理目的、处理方式等处理个人信息；

c）委托合同不生效、无效、被撤销或者终止的，受托人应将个人信息返还个人信息处理者或者予以删除，不得保留；

d）未经个人信息处理者同意，受托人不得转委托他人处理个人信息；

e）因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应向个人告知转移方的名称或者姓名和联系方式，转移方应继续履行个人信息处理者的义务，转移方变更原先的处理目的、处理方式的，应按照相关法律法规要求取得个人同意；

f）向其他个人信息处理者提供其处理的个人信息的，应向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并按属地法律法规要求取得个人同意；接收方变更原先的处理目的、处理方式的，应重新取得个人同意。

4.5 个人信息跨境

4.5.1 通用规则

个人信息处理者跨境处理个人信息，应满足以下要求：

a）制定个人信息跨境安全管理制度和操作规程，采取相应的加密、去标识化等安全技术措施，防范跨境个人信息遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；

b）应对个人信息跨境处理活动进行日志记录，个人信息跨境处理日志至少保存 3 年；

c）应识别数据跨境处理中涉及的个人信息，形成个人信息跨境处理目录，并及时更新;

d）应对被授权跨境访问或查阅个人信息的人员，建立最小授权的访问控制策略，使其只能访问或查阅职责所需的最小必要的个人信息和数据操作权限;

e）承诺接受认证机构对个人信息跨境处理活动的持续监督，包括答复询问、配合检查、服从采取的措施或做出的决定等，并提供已采取必要行动的书面证明。

4.5.2 跨境提供个人信息责任

个人信息处理者在跨境提供个人信息时，应在满足 4.5.1 要求基础上符合以下要求:

a）在跨境处理个人信息之时或之前，应向个人信息主体告知接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类、保存期限，以及个人向接收方行使个人信息权利的方式和程序等事项;

b）应按照属地法律法规要求取得个人信息主体的同意;

c）与接收方签订具有法律约束力的文件，约定个人信息跨境处理的目的、方式、范围、种类、数量、保存期限、存储地点，明确双方保护个人信息的责任和义务，并要求接收方不得将接收的个人信息转移至粤港澳大湾区之外的第三方;

d）应采取合同协议约定、向认证机构承诺、主管部门备案、定期审计接收方日志、每年开展数据出境安全风险自评估等措施，防止接收方将接收的个人信息转移至粤港澳大湾区之外的第三方。

4.5.3 跨境接收个人信息责任

个人信息处理者跨境接收个人信息，应在满足 4.5.1 要求的基础上符合以下要求:

a）应按照签订的具有法律效力文件约定的处理目的、处理方式、保护措施等跨境处理个人信息，不得超出约定处理个人信息，若接收方违反相关约定，获得的认证即被视为终止或失效;

b）当合同协议未生效、无效、被撤销、终止或者按个人信息处理者要求应当删除时，应当将个人信息返还跨境提供个人信息的个人信息处理者或者予以删除，不应保留。

5 个人信息权益保障要求

5.1 个人信息主体权利

个人信息处理者应保障个人信息主体享有下列权利，主要包括:

a）个人信息主体有权查阅、复制处理的个人信息;

b）个人信息主体发现其个人信息不准确或者不完整的，有权请求个人信息更正、补充;

c）个人信息主体有权要求对个人信息处理规则进行解释说明;

d）个人信息主体有权撤回对个人信息处理的同意;

e）有下列情形之一的，个人信息处理者应按照属地法律法规要求主动删除个人信息:

- 处理目的已实现、无法实现或者为实现处理目的不再必要;
- 停止提供产品或者服务，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法规或者违反约定处理个人信息。

5.2 个人信息处理者的责任义务

个人信息处理者应为个人信息主体行使权利提供便利条件，履行下列责任义务:

a）为个人信息主体提供查阅、更正、删除、撤回同意、拒绝处理个人信息的便捷渠道;

b）建立便捷的个人行使权利的申请受理和处理机制，及时响应个人信息主体提出的权利请求，在 40 日内或属地法律法规规定的期限内作出答复及合理解释，拒绝个人行使权利请求的应说明理由;

c）出现难以保证个人信息安全的情况时，应及时停止跨境处理个人信息，并通知相关个人信息处理者。

6 个人信息安全要求

个人信息处理者应当采取下列措施保护个人信息安全，防止跨境个人信息泄露、篡改、破坏、丢失。

a）个人信息处理者应指定个人信息保护负责人，设立个人信息保护机构，履行个人信息保护义务;

b）制定个人信息安全管理制度和操作规程，定期对相关人员进行个人信息安全教育和培训;

c）传输和存储敏感的个人信息时，应采用加密等安全措施；

d）合理限制个人信息处理的操作权限，与从事个人信息处理岗位上的相关人员签署保密协议；

e）对个人信息的重要操作设置内部审批流程，如进行批量修改、拷贝、下载等重要操作；

f）制定个人信息安全事件应急预案，定期组织内部人员进行应急演练；

g）一旦发生个人信息安全事件，应立即采取补救措施并通知相关个人信息处理者，向有关部门报告，按照有关要求通知个人信息主体，记录安全事件相关事实和影响，留存有关证据。