TC260-PG-20245A

网络安全标准实践指南

——粤港澳大湾区（内地、香港）个人信息跨境处理保护要求

(v1.0-202411)

全国网络安全标准化技术委员会秘书处

香港个人资料私隐专员公署

2024 年 11 月

本文档可从以下网址获得：
www.tc260.org.cn/

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）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。

《网络安全标准实践指南—粤港澳大湾区（内地、香港）个人信息跨境处理保护要求》（以下简称《跨境保护要求》）由网安标委秘书处和香港个人资料私隐专员公署制定，就粤港澳大湾区（内地、香港）个人信息跨境处理应遵循的基本原则和保护要求提供指引，为实施粤港澳大湾区（内地、香港）个人信息跨境安全互认提供了认证及认可依据。

本文件起草单位：中国电子技术标准化研究院、香港个人资料私隐专员公署、中国网络安全审查认证和市场监管大数据中心、北京理工大学、中央财经大学、广州南沙经济技术开发区管理委员会、国家工业信息安全发展研究中心、中国南方电网有限责任公司、华为技术有限公司、OPPO 广东移动通信有限公司、广州根链国际网络研究院有限公司、广州力挚网络科技有限公司、中科汇智（广东）信息科技有限公司、中企网络通信技术有限公司。

本文件主要起草人：杨建军、钟丽玲、范科峰、姚相振、胡影、黄宝漫、朱雪峰、李海东、任英杰、陈世翔、郝春亮、

岳熙研、洪延青、张金平、林伟杰、林小栋、孙杰、禤亮、陈彬、柯耀斌、韦宗慧、王秉政、杨晓伟、郑云文、刘文园、张汉卓、陈旭敏、郭桂福、何梦莎。

声　明

本《跨境保护要求》版权属于网安标委秘书处和香港个人资料私隐专员公署，未经双方书面授权，不得以任何方式抄袭、翻译《跨境保护要求》的任何部分。凡转载或引用本《跨境保护要求》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处、香港个人资料私隐专员公署”。

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，落实《中华人民共和国国家互联网信息办公室与香港特别行政区政府创新科技及工业局 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”）中粤港澳大湾区个人信息跨境安全认证工作，依据备忘录、内地认证文件和属地法律法规，制定本文件。粤港澳大湾区（内地、香港）个人信息处理者、接收方可以按照备忘录和相关文件要求，采取订立大湾区（内地、香港）个人信息跨境流动标准合同或者申请以大湾区（内地、香港）个人信息跨境安全互认方式（以下简称“安全互认方式”）进行大湾区内个人信息跨境流动。《促进和规范数据跨境流动规定》规定的免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形除外。

本文件规定了粤港澳大湾区（内地、香港）个人信息处理者或者接收方，在大湾区内内地和香港间通过安全互认方式进行大湾区内个人信息跨境流动应遵守的基本原则和要求。对粤港澳大湾区（内地、香港）个人信息处理者或者接收方的个人信息跨境处理活动进行安全认证（就粤港澳大湾区内内地个人信息处理者或者接收方而言）或认可（就香港特别行政区个人信息处理者或者接收方而言），依据本文件开展。

目　录

1 范围

本文件规定了粤港澳大湾区（内地、香港）个人信息处理者或者接收方，在大湾区内内地和香港间通过安全互认方式进行大湾区内个人信息跨境流动应遵守的基本原则和要求。

本文件作为粤港澳大湾区（内地、香港）个人信息跨境安全互认的认证（就粤港澳大湾区内内地个人信息处理者或者接收方而言）及认可（就香港特别行政区个人信息处理者或者接收方而言）依据，适用于粤港澳大湾区（内地、香港）个人信息处理者或者接收方，按照大湾区个人信息跨境安全互认相关文件要求，通过自愿申请大湾区个人信息跨境安全认证的方式（就粤港澳大湾区内内地个人信息处理者或者接收方而言）或自愿申请加入由香港个人资料私隐专员公署设立的“粤港澳大湾区（内地、香港）跨境个人资料转移认可名单”（就香港特别行政区个人信息处理者或者接收方而言），进行大湾区内内地和香港之间的个人信息跨境流动。被相关部门、地区告知或者公开发布为重要数据的个人信息除外。

粤港澳大湾区（内地、香港）个人信息处理者或者接收方，是指注册于（适用于组织）／位于（适用于个人）粤港澳大湾区境内部分，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，或者香港特别行政区的个人信息处理者或者接收方。

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：粤港澳大湾区内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；香港特别行政区内个人信息处理者处理的个人信息，按照香港特别行政区《个人资料（私隐）条例》的“个人资料”确定。

2.2 个人信息主体

个人信息所识别或者关联的自然人。

注：就香港特别行政区而言，亦涵盖“资料当事人”，即就个人资料而言，指属该资料的当事人的个人。

2.3 个人信息处理者

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1：就香港特别行政区而言，亦涵盖“资料使用者”，即就个人资料而言，指独自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。

注2：本文件的个人信息处理者是指个人信息跨境提供方，即跨境提供个人信息的个人信息处理者。

2.4 接收方

自个人信息处理者处跨境接收个人信息的组织、个人。

2.5 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：就香港特别行政区而言，亦涵盖个人信息的收集、持有、处理或使用(包括披露或移转)。

2.6 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。

2.7 个人信息跨境

个人信息处理者在粤港澳大湾区（内地、香港）内跨境处理个人信息。

注：本文件所称个人信息跨境主要包括：1）个人信息在大湾区内内地和香港间跨境传输（含单向、双向）；2）接收方通过查询、调取、下载、导出等方式处理存储在个人信息处理者的个人信息；3）符合《中华人民共和国个人信息保护法》第三条第二款情形，在香港特别行政区处理内地自然人个人信息等其他数据处理活动。

3 基本原则

3.1 合法、正当、诚信原则

个人信息处理者、接收方处理个人信息，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、合法的目的；

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

个人信息处理者、接收方处理个人信息，应与处理目的直接相关，限于实现处理目的所需的最小范围，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、接收方处理个人信息，应遵循公开、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 权益保障原则

个人信息处理者、接收方处理个人信息，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、接收方应采取必要措施保障个人信息的安全和保密，防止未经授权的访问或查阅以及个人信息遭到泄露、篡改、丢失、滥用。

3.6 责任明确原则

个人信息处理者、接收方应对其个人信息处理活动负责，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、接收方处理个人信息应符合属地法律法规要求，具体包括:

a）就粤港澳大湾区内内地的个人信息处理者、接收方而言，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）就香港特别行政区的个人信息处理者、接收方而言，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 个人信息收集

个人信息处理者收集个人信息，应符合以下要求，属地法律法规另有规定的除外：

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、种类；

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）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；

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；就香港特别行政区而言，处理不满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。

e）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、接收方存储、使用、加工个人信息，应符合以下要求，属地法律法规另有规定的除外：

a）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，应按照属地法律法规要求重新取得个人信息主体同意；

c）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；

d）通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式，属地法律法规未有规定的除外；

e）通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者或接收方予以说明，拒绝个人信息处理者或接收方仅通过自动化决策方式作出决定，属地法律法规未有规定的除外；

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。

f）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、接收方委托处理、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、双方的权利和义务，以及合同到期或终止时个人信息删除或返还要求，并对受托人的个人信息处理活动进行监督；

b）向其他个人信息处理者（“其他个人信息处理者”简称“接收者”）提供其处理的个人信息的，应按属地法律法规要求向个人告

知接收者的名称或者姓名、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；接收者变更原先的处理目的、处理方式的，应按照属地法律法规要求重新取得个人同意；

c）公开其处理的个人信息应按属地法律法规要求取得个人的同意，并采取去标识化等技术手段降低公开数据敏感性；处理个人自行公开或其他已合法公开的个人信息按属地法律法规要求执行。

4.5 个人信息跨境

4.5.1 通用要求

个人信息处理者、接收方跨境处理个人信息，应满足以下要求：

a）在个人信息跨境处理前，明确约定跨境个人信息的处理目的、处理方式、跨境个人信息的种类和规模、传输方式、跨境后保存地点和保存期限、个人信息向同辖区第三方提供的情况；

b）制定个人信息跨境安全管理制度，采取相应的加密、去标识化、访问或查阅控制等安全技术措施保护跨境个人信息，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、非法利用等风险；

c）对个人信息跨境处理活动进行记录，个人信息跨境处理情况记录至少保存 3 年。

4.5.2 跨境提供个人信息

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）向接收方跨境提供的个人信息应仅限于实现处理目的所需的最小范围；

b）按属地法律法规要求向个人信息主体告知接收方的名称或者姓名、联系方式，按照 4.5.1 a）约定的处理目的、处理方式、个人信息的种类、保存期限、个人信息向同辖区第三方提供的情况，以及行使个人信息权利的方式和程序等事项，属地法律法规要求不需要告知的，从其规定；

c）向接收方跨境提供个人信息前，应按照属地法律法规要求取得个人信息主体的同意，属地法律法规另有规定的除外；

d）与接收方订立具有约束力的文件，按照 4.5.1 a）约定个人信息跨境处理相关信息，明确双方保护个人信息的责任和义务，并要求接收方按照其通知或根据个人信息主体向其提出的请求在合理期限内实现个人信息主体依照个人信息处理者属地法律法规所享有的权利，以及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；

注：企业集团或从事联合经济活动的企业集团使用具有约束力的公司规则，对个人信息跨境处理进行约定，也可认为是具有约束力的文件。

e）对拟向接收方提供个人信息的活动开展个人信息保护影响评估，保存评估报告至少 3 年，重点评估以下内容：

1）个人信息处理者和接收方处理个人信息的目的、方式等的合法性、正当性、必要性；

2）对个人信息主体权益的影响及安全风险；

3）接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障跨境提供的个人信息安全。

f）对接收方个人信息跨境处理活动进行监督，如采取合同协议规则约定、定期审计个人信息跨境处理记录、开展数据出境安全风险自评估等措施，防止接收方私自向粤港澳大湾区以外的组织、个人提供接收的跨境个人信息。

4.5.3 跨境接收个人信息

接收方跨境接收个人信息，应在满足 4.5.1 要求的基础上符合以下要求：

a）应按照双方 4.5.1 a）约定和签订的具有约束力文件，处理个人信息；

b）跨境个人信息的保存期限为实现处理目的所必要的最短时间，保存期限届满的，应删除跨境接收的个人信息（包括所有备份）；

c）受个人信息处理者委托处理个人信息，委托合同未生效、无效、被撤销、终止或者按个人信息处理者要求删除的，应将个人信息删除，并向个人信息处理者提供书面说明；删除个人信息从技术上难以实现的，接收方应停止除存储和采取必要的安全保护措施之外的处理；

d）跨境业务下线或终止服务时，接收方应及时返还或者删除所接收到的个人信息（包括所有备份），并向个人信息处理者提供书面

说明；删除个人信息从技术上难以实现的，接收方应当停止除存储和采取必要的安全保护措施之外的处理；

e）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或查阅控制策略，使其只能访问或查阅职责所需的最小必要的个人信息；

f）如处理的个人信息发生或者可能发生个人信息安全事件（如个人信息遭到篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问、查阅等），应开展以下工作：

1) 及时采取适当补救措施，减轻对个人信息主体造成的不利影响；

2) 立即通知个人信息处理者，并报告相关属地监管机构，通知应包含下列事项：

- 涉及的个人信息种类、原因和可能造成的危害。
- 已采取的补救措施。
- 个人信息主体可以采取的减轻危害的措施。
- 负责处理相关情况的负责人或者负责团队的联系方式。

3) 属地法律法规要求通知个人信息主体的，通知的内容包含本项 2）中通知所含事项；

4) 记录并留存所有个人信息安全事件有关的情况，包括采取的所有补救措施。

g）不应向粤港澳大湾区以外的组织、个人提供接收的跨境个人信息；

h）如需向粤港澳大湾区内内地或香港特别行政区同辖区内的第三方提供个人信息，应同时符合以下条件：

1) 确有业务需要；

2) 已告知个人信息主体该第三方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。个人信息处理者属地法律法规要求不需要告知的，从其规定；

3) 基于个人同意处理个人信息的，应按照个人信息处理者属地法律法规要求取得个人信息主体同意；

4) 按照 4.5.1 a）约定向同辖区内的第三方提供个人信息。

i）受个人信息处理者委托处理个人信息，转委托第三方处理的，应事先征得个人信息处理者同意，要求该第三方不得超出 4.5.1 a）约定的处理目的、处理方式等处理个人信息，并对该第三方的个人信息处理活动进行监督；

j）承诺向个人信息处理者提供已遵守双方约定和具有约束力文件所需的必要信息，允许个人信息处理者对跨境处理活动进行合规审计，并为个人信息处理者开展合规审计提供便利；

k）接收方应按照个人信息处理者的通知，或者根据个人信息主体向个人信息处理者提出的请求，在合理期限内实现个人信息主体依照个人信息处理者属地法律法规所享有的权利；

l）接收方拒绝个人信息主体请求的，应告知个人信息主体其拒绝的原因，以及个人信息主体向个人信息处理者或者接收方属地监管机构提出投诉和寻求司法救济的途径。

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、接收方应按属地法律法规保障个人信息主体权利，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，属地法律法规未有规定的除外；

d）针对处理目的已实现、无法实现或者为实现处理目的不再必要的个人信息，以及违反属地法律法规或违反约定处理的个人信息，个人信息主体有权请求删除个人信息，属地法律法规未有规定的除外。

5.2 个人信息权益保障

个人信息处理者、接收方应按属地法律法规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、复制、更正、补充、删除、拒绝处理个人信息的便捷渠道，属地法律法规未有规定的除外；

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）如属地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）发现或被内地监管部门告知影响或者可能影响中华人民共和国境内个人、组织的合法权益，危害国家主权、安全和发展利益的，应及时停止中华人民共和国境内的个人信息处理者或接收方所作的个人信息跨境流动或处理，并通知相关个人信息处理者或接收方。

6 个人信息安全要求

个人信息处理者、接收方应采取下列措施保护个人信息安全，防止跨境个人信息遭到泄露、篡改、破坏、丢失、滥用等风险。

a）指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保护措施等进行监督；

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，并在有需要保密的情况下（如个人信息属敏感的个人信息时），与从事个人信息处理岗位上的相关人员签署保密协议；

注：敏感的个人信息包括生物识别、宗教信仰、特定身份、金融账户、医疗健康、行踪轨迹以及未成年人个人信息等敏感的个人信息。

e）采取加密、去标识化、身份鉴别、访问或查阅控制、安全审计等安全技术措施，防止未经授权的访问或查阅以及个人信息遭到泄露、篡改、丢失；

f）制定个人信息安全事件应急预案，发生或者可能发生个人信息遭到篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问、查阅的，应立即采取补救措施，并通知相关属地监管机构和按属地法律法规要求通知个人。

说明：本文件规定不影响内地履行个人信息保护职责的部门和香港个人资料私隐专员公署在职责范围内依法加强个人信息保护和监督管理工作，包括处理与个人信息保护有关的投诉、举报，调查、处理违法个人信息处理活动等。

参考文献

[1] 《中华人民共和国数据安全法》

[2] 《中华人民共和国个人信息保护法》

[3] 香港特别行政区《个人资料（私隐）条例》（香港法例第486章）

[4] 香港个人资料私隐专员公署跨境资料转移指引：《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》

[5] 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》

[6] GB/T 35273-2020 信息安全技术 个人信息安全规范

[7] TC260-PG-20222A 网络安全标准实践指南—个人信息跨境处理活动安全认证规范