澳門科技大學
MACAU UNIVERSITY OF SCIENCE AND TECHNOLOGY

澳门科技大学

科研数据跨境传输活动管理

安全保护规则

2022 年 12 月

目录

1. 背景介绍

澳门科技大学携手珠海澳科大科技研究院（“规则约束成员”）积极响应国家粤港澳大湾区发展的大局，依托澳门科技大学下一代互联网国际研究院已有教学科研

基础，在广州市南沙区设立“下一代互联网国际研究院南沙分院”，并通过联合申报开展科研项目等形式，深度推进粤澳两地联合科研、人才培养、国际学术交流方面的紧密联系。

为确保科研数据中个人信息在粤澳两地依法有序地自由流动和合理地高效利用，以及出境的科研项目相关的个人信息保护和安全，规则约束成员搭建了澳门科技大学科研数据跨境流动安全管理平台（以下简称为“澳科大科研数据跨境流动安全管理平台”），共同制定了安全保护规则（以下简称为“本规则”），并签署安全保护协议，同意本规则在成员间的适用，接受本规则对成员的约束。

本规则及配套制度为规则约束成员在保障出境个人信息安全方面所承诺的最低标准，规则约束成员有权就个人信息安全实施更具保护性的制度和措施。

本安全保护规则及配套制度中也涉及非个人信息的一般数据的原则性规定，以便建立规则约束成员的全面规范的数据安全体系，但非个人信息的一般数据可以不适用本规则和配套制度的认证流程。重要数据的跨境传输应根据相关法律法规规定向网信部门申请出境安全评估。

2. 术语和定义

本规则及配套制度和安全保护协议中下列术语的含义：

(1) 数据：是指任何以电子方式或其他方式对信息的记录。
(2) 科研数据：是指以电子方式记录的在科学研究活动中收集、观察、生成或创建的任何原始信息及其衍生信息。其类型包括但不限于音频、视频、图片、表格、文字等。
(3) 个人信息：是指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，不包括匿名化处理后的信息。
(4) 敏感个人信息：是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。
(5) 一般数据：是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人、组织合法权益造成危害，但不会危害国家安全、公共利益的数据。
(6) 重要数据：是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。具体应参考中国境内相关地区和部门制定的重要数据目录。
(7) 处理：是指对数据的收集、存储、使用、加工、传输、提供、公开、删除等。
(8) 数据处理者：是指在数据处理活动中自主决定处理目的、处理方式的规则约束成员。

(9) 数据出境：是指数据处理者向境外提供在中华人民共和国境内运营中收集和产生的数据。
(10) 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、处理方式的规则约束成员；
(11) 境外接收方：位于中华人民共和国境外并自个人信息处理者处接收个人信息的规则约束成员；
(12) 个人信息主体：是指个人信息所标识或者关联的自然人。
(13) 去标识化：是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。
(14) 匿名化：是指个人信息经过处理无法识别特定自然人且不能复原的过程。

3. 适用范围

3.1 数据范围

本规则适用于规则约束成员为申报、开展中国境内和/或澳门有关部门和/或机构的科研项目所必需而进行的科研数据处理活动，包括：

(1) 科研项目管理类数据：科研人员数据、科研设备数据、数字化工具数据、流程管理数据、财务管理数据、采购管理数据、档案管理数据；
(2) 科研文献和资料类数据：文献数据、资料数据；
(3) 科研实验类数据：网络实验数据、人工智能实验数据；
(4) 科研成果类数据：学术论文数据、学术报告数据、知识产权数据。[1]

本规则只适用于科研数据中个人信息的跨境传输要求，对于科研数据中重要数据的跨境传输应根据相关法律法规规定向网信部门申请出境安全评估。本规则使用的跨境处理个人信息情况参见规则约束成员签订的安全保护协议的“附录一：出境个人信息概况”。

3.2 地域范围

本规则适用于中国境内的规则约束成员向中国境外的规则约束成员提供和传输数据。

4. 个人信息处理原则

规则约束成员应承诺并保证对个人信息的处理活动应遵守当地适用的法律法规和监管部门的规定和要求。若境外法律法规不能满足本规则制定标准的，规则约

[1] 关于数据范围的更加详细列表规定在规则约束成员共同根据《数据的类别识别指南》制定的《科研数据分类分级清单》中，该清单经规则约束成员的个人信息保护管理机构（数据安全委员会）审批后发布实施。

束成员应确保遵守本规则处理个人信息，除非当地法律对个人信息有更具保护性的规定而优先适用（请参见本规则第 14 部分）。

若适用的当地法律法规阻碍规则约束成员履行其在本规则下的责任和义务，或者对其遵守本规则有严重不利影响，规则约束成员应按照《数据安全管理角色与流程指南》进行处理。

4.1 合法、正当和必要性原则

4.1.1 规则约束成员处理个人信息应当遵守合法、正当和必要原则，且不通过误导、欺诈、胁迫等方式处理个人信息。

4.1.2 规则约束成员处理个人信息应至少具备符合下列情形之一：

(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) 依照适用法律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；
(7) 适用法律法规规定的其他情形。

4.1.3 规则约束成员处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

4.1.4 规则约束成员收集理个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

4.2 目的限制原则

规则约束成员使用个人信息时，不应超出与收集个人信息时所声称的目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，应再次征得个人信息主体明示同意。

4.3 公开、透明原则

4.3.1 规则约束成员处理个人信息应当遵守公开、透明原则，在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人信息主体告知处理活动相关的信息，包括但不限于以下事项：

(1) 个人信息处理者的基本情况，包括主体身份、联系方式；

(2) 收集、使用个人信息的处理目的，以及各处理目的下分别收集的个人信息类型。涉及个人敏感信息的，需明确标识或突出显示；
(3) 个人信息收集方式、存储期限、涉及数据出境情况等个人信息处理规则；
(4) 对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任；
(5) 个人信息主体的权利和实现机制，如查询方法、更正方法、删除方法、注销账户的方法、撤回授权同意的方法、获取个人信息副本的方法、对信息系统自动决策结果进行投诉的方法等；
(6) 提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响；
(7) 遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施，必要时可公开数据安全和个人信息保护相关的合规证明；
(8) 处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联 络方式。

4.3.2 前述事项发生变化时，应及时将变更部分告知个人信息主体。

4.4 个人信息准确性和完整性

规则约束成员处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

4.5 告知同意

规则约束成员基于个人同意处理个人信息的，该同意应当由个人信息主体在充分知情的前提下自愿、明确作出。适用法律法规规定处理个人信息应当取得个人信息主体单独同意或者书面同意的，从其规定。

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，规则约束成员应当重新取得个人信息主体的同意。

4.6 个人信息存储时间最小化

除适用的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。超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理。

4.7 个人信息对外提供

4.7.1 规则约束成员向另一方提供个人信息的，应当根据本规则规定签订有法律约束力和执行力的安全保护协议。

4.7.2 规则约束成员向不包括规则约束成员在内的第三方提供个人信息的，应当向个人信息主体告知接收方的名称或者姓名和联系方式、处理目的、处理方式和个人信息的种类，并取得个人信息主体的单独同意，法律法规另有规定的除外；

4.7.3 应准确记录和存储个人信息对外提供情况，包括对外提供的日期、规模、目的以及数据接收方基本情况等；

4.7.4 与第三方签署书面合同，合同应明确以下事项：

(1) 对外提供和第三方处理个人信息的目的、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；
(2) 第三方应协助规则约束成员履行个人信息保护相关义务，包括但不限于响应个人信息主体权利请求，发生个人信息安全事件时及时告知数据处理者，协助数据处理者进行个人信息保护影响评估；
(3) 当合同不生效、无效、被撤销或者终止时，数据接收方应根据数据处理者的要求删除或者返回个人信息；
(4) 第三方应配合规则约束成员对其进行安全审计以及对其数据安全管理情况的随时检查，包括但不限于按照数据处理者的要求提供数据处理设施、数据文档和处理所需的文件，并按数据处理者的要求及时处理审计和检查中发现的数据违规使用、滥用等情况。

4.8 个人信息委托处理

4.8.1 规则约束成员委托第三方处理个人信息的应严格评估和甄选受托方，确保其拥有实施和维持必要的技术和管理措施的能力来按照本规则的要求处理个人信息；

4.8.2 应准确记录和存储受托方处理个人信息的情况，并对受托方进行监督，包括但不限于：通过合同方式规定受托者的责任和义务、对受托者进行审计；

4.8.3 与受托方签署书面合同，合同应明确以下事项：

(1) 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;
(2) 根据数据处理者的指示处理个人信息，且不得超过数据处理者自身所获得的授权范围；
(3) 未经数据处理者事先书面同意不得进行转委托，并确保分包方受制于不低于数据处理者与受托方约定的个人信息保护要求。受托方应对分包商的全部行为向数据处理者承担全部责任。同时，若受托方位于境外，则应满足本规则中有关【个人信息出境再转移】部分的要求。
(4) 受托方应协助委托方履行个人信息保护相关义务，包括但不限于响应个人信息主体权利请求，发生个人信息安全事件时及时告知委托方，协助数据处理者进行个人信息保护影响评估；

(5) 当委托合同不生效、无效、被撤销或者终止时，受托方应根据数据处理者的要求删除或者返回个人信息；
(6) 受托方应配合委托方对其进行安全审计以及对受托方的数据安全管理情况的随时检查，包括但不限于按照数据处理者的要求提供数据处理设施、数据文档和处理所需的文件，并按数据处理者的要求及时处理审计和检查中发现的数据违规使用、滥用等情况。

4.9 个人信息出境再转移

作为境外接收方的规则约束成员向境外第三方再转移个人信息的，不管是对外提供还是委托处理，除应当遵守本规则关于对外提供和委托处理的要求，还应当满足以下条件之一：

(1) 与该第三方签署合同，明确约定其遵守与本规则类似的个人信息处理原则采取不低于本规则的个人信息保护措施。
(2) 依照《个人信息保护法》第四十条的规定通过中国网信部门组织的安全评估；
(3) 按照中国网信部门的规定经专业机构进行个人信息保护认证；
(4) 按照中国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；
(5) 中国法律、行政法规或者中国网信部门规定的其他条件。

4.10 公开披露

除取得个人信息主体单独同意外，规则约束成员不得公开其处理的个人信息。

4.11 公开个人信息处理

规则约束成员可在合理范围内处理个人信息主体自行公开过其他的个人信息；个人信息主体明确拒绝的除外。规则约束成员处理已公开的个人信息，对个人权益有重大影响的，应当依照本规则规定取得个人信息主体同意。

4.12 敏感个人信息处理规则

(1) 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处理敏感个人信息。
(2) 处理敏感个人信息应当取得个人的单独同意；适用法律法规规定处理敏感个人信息应当取得书面同意的，从其规定。
(3) 规则约束成员处理敏感个人信息的，除本规则第 4.3 条规定的事项外，还应当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，相关法律法规规定可以不向个人告知的除外。
(4) 规则约束成员处理不满十四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同意，并制定专门的个人信息处理规则。

(5) 适用法律法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

4.13 个人信息安全

4.13.1 技术和管理措施

规则约束成员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，采取下列防止确保个人信息处理活动未经授权的访问以及个人信息泄露、篡改、丢失：

(1) 制定内部管理制度和操作规程；
(2) 对个人信息实行分类管理；
(3) 采取相应的加密、去标识化等安全技术措施；
(4) 合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；
(5) 适用法律法规规定的其他措施。

本规则约束成员为防范个人信息出境安全风险所采取的技术和管理措施参见安全保护协议“附录二：防范个人信息出境风险采取的技术和管理措施”。

4.13.2 发生或者可能发生个人信息泄露、篡改、丢失等个人信息安全事件的，规则约束成员应当按照《数据安全事件处置指南和应急响应预案》采取补救措施，并通知相关监管部门和个人信息主体。

4.13.3 当境外接收方的实质控制权或者经营范围发生实质性变化，或者所在国家、地区法律环境发生变化导致难以保障个人信息安全或无法履行本《安全保护规则》、相关法律法规所提出的要求时，规则约束成员应当按照《数据安全事件处置指南和应急响应预案》采取安全措施，并通知相关监管部门和数据处理者。

5. 个人信息主体权利

作为数据处理者的规则约束成员应当保障个人信息主体以下权利：

5.1 知情权、决定权、限制权和拒绝权

个人信息主体对其个人信息的处理享有知情权、决定权，有权限制或者拒绝数据处理者对其个人信息进行处理。同时，个人信息主体有权要求数据处理者对其个人信息处理规则进行解释说明。

5.2 查阅、复制权

个人信息主体有权向数据处理者查阅、复制其个人信息，除适用法律法规另有规定外。

5.3 转移权

个人信息主体请求将指定的个人信息转移至其指定的数据处理者，符合中国网信部门的或者适用法律法规以及当地监管部门规定条件的，数据处理者应当提供转移的途径。

5.4 更正、补充权

个人信息主体发现其个人信息不准确或者不完整，有权要求数据处理者更正和补充。

5.5 删除权

5.5.1 在满足下述情形之一时，若数据处理者未主动进行删除的，个人信息主体有权请求删除：

(1) 处理目的已实现、无法实现或者为实现处理目的不再必要；
(2) 数据处理者停止提供产品或者服务，或者保存期限已届满；
(3) 个人信息主体撤回同意；
(4) 数据处理者违反适用法律法规或者违反约定处理个人信息；
(5) 适用法律法规规定的其他情形。

5.5.2 适用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，数据处理者应当停止除存储和采取必要的啊安全保护措施之外的处理。

5.6 撤回同意权

数据处理者基于个人信息主体“同意”这一法定合理理由收集处理的个人信息，个人信息主体有权撤回该同意。

5.7 注销权

个人信息主体有权注销其注册的数据处理者运营的网站、APP、微信公众号、小程序等账户。

5.8 近亲属对去世个人信息主体的个人信息的权利

个人信息主体去世后，其近亲属为了自身的合法、正当利益，可以对去世个人信息主体的相关个人信息行使本规则规定的查阅、复制、更正、删除等权利；死者生前安排的除外。

6. 一般数据处理原则

规则约束成员应承诺并保证对科研数据中非个人信息的一般数据的处理活动应遵守当地适用的法律法规和监管部门的规定和要求。若境外法律法规不能满足本规则制定标准的，规则约束成员应确保遵守本规则处理一般数据，除非当地法律对一般数据有更具保护性的规定而优先适用（请参见本规则第 14 部分）。

若适用的当地法律法规阻碍规则约束成员履行其在本规则下的责任和义务，或者对其遵守本规则有严重不利影响，规则约束成员应按照《数据安全管理角色与流程指南》进行处理。

6.1 数据收集

数据处理者收集数据应当遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据。

数据收集过程中，应当根据数据安全级别采取相应的安全措施，并对数据收集的时间、类型、数量、频度、流向等进行记录。

6.2 数据存储

数据处理者应当依据法律规定或者与相关数据权利人约定的方式和期限存储数据。

6.3 数据使用加工

数据处理者利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。

6.4 数据传输

数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。

6.5 数据提供

数据处理者提供数据，应当明确提供的范围、类别、条件、程序等，并与数据获取方签订数据安全协议。

6.6 委托处理

数据处理者委托他人开展数据处理活动的，应当通过签订合同协议等方式，明确委托方与被委托方的数据安全责任和义务。

除适用法律法规另有规定外，未经数据处理者同意，受托方不得进行转委托或者将数据提供给第三方。

6.7 数据公开

数据处理者应当在数据公开前分析研判可能对公共利益、国家安全产生的影响，存在重大影响的不得公开。

6.8 数据销毁

数据处理者应当建立数据销毁策略和管理制度，明确销毁对象、流程和技术等要求，对销毁活动进行记录和留存。相关数据权利人或其他个人和组织依据法律规定、合同约定等请求销毁的，数据处理者应当销毁相应数据。

6.9 数据出境再转移

作为境外接收方的规则约束成员向境外第三方再转移数据的，应当遵守本规则关于数据对外提供和委托处理的要求。

规则约束成员发生分立、解散、破产、合并等情形进行个人信息再转移的，应当遵守本规则关于数据对外提供和委托处理的要求。

6.10 数据安全监测与应急管理

规则约束成员应当开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险。在发生数据安全事件后，应当根据《数据安全事件处置指南和应急响应预案》，及时开展应急处置。

7. 重要数据识别和出境

7.1 作为数据处理者的规则约束成员应根据中国境内相关地区、部门和行业制定的重要数据目录，对科研数据中的重要数据进行识别和划分，并在识别重要数据后按照有关要求向中国境内主管监管部门备案。备案内容发生重大变化的，包括但不限于处理数据的目的、范围、类型及数据安全防护措施等，应按照有关要求及时报备变更情况或重新进行备案。

7.2 作为境内个人信息处理者的规则约束成员向境外规则约束成员传输和提供重要数据的，应根据相关法律法规规定向网信部门申请出境安全评估。

8. 合规证明机制

规则约束成员应当通过以下机制对其遵守适用法律法规和本规则的规定进行证明：

8.1 数据处理活动记录

规则约束成员不管是作为数据处理者还是受托方，应建立、维护和更新数据处理活动记录，记录内容应包括所涉及的个人信息和数据类型、数量、来源；数据处理目的、使用场景，以及委托处理、对外提供、公开披露以及出境等情况；与个人信息处理活动各环节相关的信息系统、组织和人员以及权限管理。

数据处理活动应以书面形式记录，包括电子形式，并妥善保存，以随时供监管部门要求、问询和调查。

8.2 个人信息保护影响评估

8.2.1 有下列情形之一的，作为数据处理者的规则约束成员应当事前进行个人信息保护影响评估，并记录相关处理活动，形成个人信息保护影响评估报告：

(1) 处理敏感个人信息；

(2) 委托处理个人信息、向其他数据处理者提供个人信息、公开个人信息；
(3) 向境外提供个人信息；
(4) 其他对个人权益有重大影响的个人信息处理活动。

对于第（3）项所列的向境外提供个人信息的个人信息保护影响评估应按照《个人信息出境保护指南》中关于个人信息出境场景下个人信息保护影响评估的相关规定开展。

8.2.2 个人信息保护影响评估应当包括下列内容：个人信息的处理目的、处理方式等是否合法、正当、必要；对个人权益的影响及安全风险；所采取的保护措施是否合法、有效并与风险程度相适应。

8.2.3 个人信息保护影响评估报告和处理情况记录应当至少保存三年。

9. 安全保护规则实施保障

9.1 人员培训

9.1.1 规则约束成员应当将为长期或者定期处理个人信息和其他科研数据的教职工、学生和其他人员以及参与开发处理个人信息和其他科研数据的工具、IT系统的教职工、学生和其他人员定期举办个人信息保护和数据安全培训，提高教职工、学生和其他人员的个人信息保护和数据安全意识。

9.1.2 培训课程由规则约束成员根据适用的法律和除了介绍适用法律法规和本规则对个人信息和其他科研数据的基本处理原则外，还应当分享案例进行具体说明。

9.1.3 规则约束成员应当采取考核等措施确保培训效果。此外，规则约束成员应明确培训的周期，以及在科研项目启动时，对科研项目主要负责人和其他相关人员进行个人信息保护和数据安全培训。

9.2 数据治理架构

规则约束成员设立数据安全委员会（个人信息保护机构）总体负责安全保护协议及安全保护规则的监督和执行。数据安全委员会由五（5）名委员组成，其中三（3）名为董事委员，两（2）名为咨询委员。董事委员由各校区/院区分管数据安全的校领导或院领导担任，咨询委员由各校区/院区科研项目数据管理相关负责人担任。

规则约束成员的数据保护官作为个人信息保护负责人，负责安全保护规则以及配套制度在成员内部的具体执行和监督。数据保护官由各规则约束成员向数据安全委员会提名，数据安全委员会通过后，由各规则约束成员任命。数

据保护官就安全保护规则及其配套制度在成员内部的实施向数据安全委员会报告工作。

规则约束成员下属各个院系或负责科研项目申报的行政部门应指定专人负责本院系或部门的数据安全工作并作为与数据保护官对接的联络人（以下简称为“数据保护联络人”）。具体科研项目在申报和开展过程中也应指定项目主要参与人员作为数据保护联络人，该数据保护联络人应为规则约束成员的教职工、学生等人员。

关于数据安全委员会、数据保护官以及数据保护联络人的职责范围以及工作流程请参见《数据安全管理角色与流程指南》。

负责处理个人信息保护相关事务的个人信息保护机构的名称或者代表、个人信息保护负责人、数据保护联络人的姓名、联系方式等依据法律相关要求报送履行个人信息保护职责的部门。

9.3 审计

9.3.1 为确保规则约束成员遵守本规则，规则约束成员应定期按照《安全认证审计制度》进行审计。审计内容包含了本规则所有重要内容以及配套制度。

9.3.2 各规则约束成员安全认证审计工作由各自的数据保护官负责组织开展，最终的审计报告提请安全委员会审批。关于数据保护官履行安全保护规则的职责的审计工作应当由各规则约束成员的内部审计人员/机构或外部专业机构来实施。

9.3.3 规则约束成员应向中国境内的相关监管部门提交安全保护规则的年度审计报告，在监管部门要求时，也可由监管部门对规则约束成员就个人信息保护和数据安全进行审计。在监管部门要求由其进行审计的情况下，各规则约束成员应积极配合监管部门的工作。

10. 本规则的公开

各规则约束成员应采取一切适当和必要的措施向相关个人信息主体以及数据权利人告知本规则以及配套制度（内部非公开文件除外）以及为个人信息主体提供便捷的访问途径，例如在校园内网或科研项目申报网站上发布，或者在教职工和学生申报科研项目时由数据保护联络人进行书面（包括纸质和电子形式）告知等。

11. 第三方受益人权利

11.1 当任一规则约束成员违反本规则的以下原则规定时，个人信息主体可向境内的有关监管部门提起申诉或者向有管辖权的法院提起诉讼请求救济或者要求损害赔偿：

（1） “4.个人信息处理的基本原则”；
（2） “5.个人信息主体权利”；
（3） “8.合规证明机制”；
（4） “9.3 审计”中关于监管部门要求审计的规定；
（5） “10.本规则的公开”；
（6） “12.申诉和投诉流程”；
（7） “13.责任和管辖权”；
（8） “14.法律适用冲突”；
（9） “15.与监管部门的合作机制”；

11.2 第三方受益人权利不适用于就规则约束成员内部关于本规则实施保障的相关内容，例如人员培训、审计、数据治理架构、安全保护规则更新机制等。

12. 申诉和投诉流程

12.1 个人信息主体申诉处置流程

个人信息主体有权向各规则约束成员行使本规则规定的各项权利，也有对规则约束成员处理个人信息进行投诉的一般权利。若个人信息主体就规则约束成员对其的权利请求或投诉的回复不满意的，还拥有向各规则约束成员的数据保护官提起申诉，或者向中国境内的有关监管部门申诉以及向依法人民法院提起诉讼的权利。

规则约束成员应按照《科研项目相关人员申诉处置指南》的处置流程和《数据安全管理角色与流程指南》的工作流程处理个人信息主体的权利请求、投诉和申诉。

12.2 数据安全投诉流程

规则约束成员应建立数据安全投诉处理机制，按照《数据安全管理角色与流程指南》的工作流程处理关于非个人信息的一般数据安全的投诉。

12.3 公开数据保护官联系方式

各规则约束成员应公开数据保护官和数据保护联络人的联系方式，以接收个人信息主体的权利请求、投诉和申诉以及数据安全投诉。

13. 责任和管辖权

13.1 若规则约束成员违反本规则导致个人信息主体、数据权利人以及其他相关方受损，该规则约束成员应当在自己的责任范围内对其他规则约束成员、境内监管部门、个人信息主体和相关数据权利人以及其他相关方的损害负责，并立即采取必要的补救措施以及就其违反安全保护规则行为导致的损害进行赔偿。

13.2 个人信息出境或者再转移之后接收个人信息的数据进口方违反安全保护规则导致个人信息主体遭受损失的，相关境内个人信息处理者应对个人信息主体承担损害赔偿责任。个人信息主体向监管部门提起申诉或者向法院提起诉讼的，境外接收方应就该等申诉或诉讼委派其数据保护官、律师或其他专业人员进行辩护、抗辩或提起反诉，并有权要求境外接收方全力配合。若在境外接收方的配合协助下，境内个人信息处理者未能证明数据进口方遵守安全保护规则，并就个人信息主体遭受的任何损失进行赔偿或者被监管部门行政处罚的，境外接收方应就境内个人信息处理者因境外接收方违反安全保护规则的行为而遭受的任何成本、损害、费用或损失进行赔偿。

13.3 为本条款目的，个人信息主体和相关数据权利人可向境内个人信息处理者所在地法院提起诉讼请求救济或者要求损害赔偿。

14. 法律适用冲突

规则约束成员应遵守任何适用的当地法律法规关于个人信息和数据处理的规定，若当地的法律法规不能满足本规则制定标准的，规则约束成员应确保遵守本规则处理个人信息和其他科研数据，除非当地法律法规对个人信息和其他科研数据有更具保护性的规定，在这种场景下，应当优先适用当地法律法规。

当境外规则约束成员因为当地适用的法律法规规定不能适用本规则，或者有合理理由认为当地适用的法律法规阻止其履行本规则的义务或者对其遵守本规则有严重不利影响的，应按照《数据安全管理角色与流程指南》报告数据安全委员会，进行调查评估，并向境内监管部门报告。

15. 与监管部门的合作机制

15.1 规则约束成员应指派数据保护官与境内监管部门就规则约束成员实施安全保护协议和安全保护规则的相关问题进行沟通，接收境内监管部门的问询和调查。

15.2 规则约束成员应在年度审计报告的基础上撰写安全认证年度报告，并向境内监管部门提交。

15.3 境内监管部门就安全保护规则的解释、适用和实施提出的意见、建议和要求，规则约束成员应当采纳和遵守。

15.4 关于与监管部门合作机制的具体流程请参见《数据安全管理角色与流程指南》。

16. 规则的更新

关于本规则及配套制度的更新流程请参见《数据安全管理角色与流程指南》。

17. 生效日期和期限

本规则应在规则约束成员签署的安全保护协议生效之日起生效，并在以下条件时终止（1）满足安全保护协议规定的条件终止；或者（2）数据安全委员审议通过终止安全保护规则并向内地监管部门报告。