**数据共享附录（供应商数据）**

**修订日期：2024年3月12日**

就本数据共享附录 (“DSA”) 而言，签订合同或引用本 DSA 的其他形式的协议（“协议”）的 Merck Sharp & Dohme LLC 实体或关联方应称为“公司”，协议的所有其他方应统称为  
“供应商”。公司和供应商各自为“一方”，合称为“双方”。

背景

1. 双方签订本协议，并可能与本协议一起签订一项或多项采购订单或任务订单、项目协议、  
   项目计划附录、工作说明书、工作订单或其他服务条款（均称为“工作说明书”），以规范其中预计提供的服务（“数据共享目的”）。
2. 双方希望对协议条款进行补充，以确保所有与协议相关的个人信息共享均遵守数据保护法，  
   并明确双方各自作为此类数据的独立控制者。

双方同意：

1. *数据共享活动*。对于与本协议相关的个人信息处理，共享的主题、性质、目的和持续时间、  
   相关数据主体的类别以及个人信息的类别均在协议中标题为“数据处理详细信息”的附件中  
   具体说明。
2. *适用范围*。本 DSA 的条款适用于协议下的每份工作说明书，除非该工作说明书另有规定。
3. *供应商义务*。在处理与本协议相关的个人信息时，供应商应：
   1. 遵守数据保护法和供应商在本 DSA 下的义务，如果供应商无法履行这些义务，供应商应立即通知公司，并采取公司认为必要的所有合理且适当的措施以纠正不合规行为。
   2. 提供所有必要的通知并从数据主体处获得所有必要的同意，以确保公司有权将个人信息用于数据共享目的。
   3. 对其员工、关联方、代理、分包商和其他代表的所有作为或不作为承担全部责任。
   4. 实施并维护合理且适当的书面信息安全和隐私计划，其中应包含与本协议中共享的个人信息的性质相应的物理、技术和组织措施，这些措施应达到或超过良好的行业惯例（或附录 1 中可能要求的更高标准），并合理防止个人数据泄露，包括以足以满足本 DSA 要求的方式对所有负责处理个人信息的人员进行培训。
   5. 遵守公司要求的所有合理且适当的必要措施，以便供应商和公司遵守数据保护法和本   
      DSA 规定的各自义务。
   6. 供应商确认并同意，签订本 DSA 即表明其理解本 DSA 中规定的限制并将遵守这些限制。
4. *赔偿*。在不限制本协议或其他协议项下公司的任何权利或权益或供应商的义务的情况下，  
   对于因供应商处理与本协议有关的个人信息而导致供应商个人数据泄露，从而导致受补偿方遭受任何损失、损害、罚款、成本或费用（包括法律费用和支出），供应商应向公司及其关联方以及其各自的管理人员、董事、员工、承包商、临时工、分包商、代理和其他代表  
   （均称为“受偿方”）进行赔偿。本节项下的任何责任均应遵守本协议中适用的责任限制或免责条款，除非该责任是由于供应商的过失或故意不当行为造成，在这种情况下，任何限制或免责条款均不适用。
5. *定义*
   1. “数据保护法”是指任何适用的数据保护、数据安全或隐私法，包括但不限于（在此类法律适  
      用的范围内）《欧盟通用数据保护条例》及与之相关的任何国家实施立法、《健康保险流通和责任法案》、《加州隐私权法案》以及任何其他国家、州、联邦、省或地区数据保护、  
      数据安全或隐私法。
   2. “个人信息”是指与本协议相关、与已识别或可识别身份的个人相关的任何数据，包括能识别特定个人身份的数据，或能够用于识别、定位、追踪或联系个人的数据。个人信息包括直接可识别身份的信息，例如姓名、身份证号码或唯一职位名称，以及间接可识别身份的信息，例如出生日期、唯一移动或可穿戴设备标识符、可用于识别家庭身份的信息、电话号码、  
      密钥编码数据、在线标识符（例如 IP 地址）或个人活动、行为或偏好，还包括根据数据保  
      护法构成“个人数据”的任何数据。
   3. “处理”是指对个人信息或个人信息集执行任何操作或一系列操作，包括但不限于通过自动化  
      方式，例如收集、记录、组织、构建、存储、访问、改编或更改、检索、咨询、使用、通过传输、传播或以其他方式提供、评估、分析、报告、共享、调整或组合、限制、删除或销毁。
   4. “个人数据泄露”是指被传输、存储或以其他方式处理的个人信息的意外或非法销毁、丢失、  
      变更、未经授权的披露或访问。
   5. “标准合同条款”是指欧盟委员会于 2021 年 6 月 4 日发布的有关向未经欧盟委员会评估为个人数据提供充分保护的第三国传输个人数据的标准合同条款，条款可能会不时更新。
   6. 如果这些定义限制或缩小了数据保护法中相关定义的范围，则应扩展该定义以符合数据保护法中的定义。
   7. 如果本节未给出定义，则术语应以符合所有适用的数据保护法的方式进行解释。
6. *解读*。
   1. 本 DSA 中使用但未定义的术语应具有本协议其他条款中规定的含义。
   2. 词语“包括”和“包含”应解释为包括但不限于。
   3. 在履行《服务协议》和本DSA下的义务时，双方承认MSD及其附属公司的公司政策要求MSD的业务应在适用的数据保护法（包括欧盟《通用数据保护条例》）的文字和精神范围内进行。如果双方不受相同数据保护法的约束，预期双方应遵守任何此类法律中所有合理相关的数据保护标准。
   4. 本协议下的数据共享目的而言，供应商可能会处理公司一个或多个关联方的个人信息。  
      在这种情况下，公司的任何关联方均应被视为个人信息的“控制者”和本 DSA 的第三方受益人，并有权依赖和执行本 DSA 赋予公司的所有权利和保护措施，无论该关联方是否被指定为本协议或本 DSA 的一方。
   5. 本 DSA 特此纳入本协议，并构成本协议的一部分。
   6. 如果协议条款与本 DSA 之间存在任何冲突，则以本 DSA 条款为准，除非协议条款对与协议相关的个人信息的保护性更强，在这种情况下，以保护性更强的协议条款为准。
   7. 如果本 DSA 的条款与标准合同条款之间存在任何冲突，则以标准合同条款为准。
   8. 除本协议明确修订，否则本协议的条款仍具有完全效力。
   9. 如果本 DSA 以英文和其他语言起草，当英文文本与其他语言文本存在差异时，应以英文文本为准。
   10. 本 DSA 中的章节标题和其他标题仅供参考，不构成本 DSA 的一部分，也不影响本 DSA 的含义或解释。
   11. 本 DSA 的附件和附录应被视为本 DSA 的组成部分，其程度与本 DSA 中逐字列出的相同。
   12. 本 DSA 的条款是可分割的。如果任何短语、条款或规定全部或部分无效或不可执行，则此类无效性或不可执行性仅影响此类短语、条款或规定，本 DSA 的其他部分仍具有完全效力。
   13. 本 DSA 管辖与数据共享目的相关的任何个人信息的处理，并对适用于数据共享目的的协议条款进行补充，除非公司和供应商已签订适用于某些数据共享目的的另一份 DSA。
   14. 本 DSA 可以签订任意数量的副本，所有副本共同构成一份相同的协议。任何一方均可通过签署此类副本来签订本 DSA。
   15. 本 DSA 构成双方就本 DSA 主题达成的完整协议，并（在法律允许的范围内）取代双方此前就该主题达成的所有陈述或口头或书面协议，但本 DSA 中的任何内容以及双方均不得试图免除欺诈性陈述的任何责任。
   16. 本协议中的管辖法律和管辖权条款将适用于本 DSA。
7. *更新限制*。
   1. 当各方续签、修改、在协议下发出新的工作声明或以任何方式修改协议或协议下的任何工作声明时（“触发事件”），位于<https://www.msdprivacy.com/privacyterms/> 的“Data Sharing Addendum (Supplier Data)”下的最新文档将取代此DSA的条款，直到下一个触发事件发生，除非在触发事件发生后的30天内提出异议。尽管有上述规定，可能存在需要立即修改本DSA条款的情况，这种修改只能出于7(b)中阐述的理由，并且只能在确保任何新的或修改的条款仅限于为了遵守新的适用数据保护法律、案例法或相关数据保护机构发布的指导而必要的条款之后，以诚信的方式进行。
   2. 如果发生以下任何情况，各方立即同意上述地址发布的最新条款，除非在公司通知新条款后的30天内，所有请求接收通知的实体在[privacy\_updates@msd.com](mailto:privacy_updates@msd.com)提出异议：  
      1. 适用的数据保护法已以现有DSA的合同条款不足以满足更新后的法律要求的方式更新，
      2. 适用的数据保护法发生变化，且各方由于法律变化有合理且正当的利益修改这些条款，例如并不限于，去除不再必要的要求，或
      3. 有新的案例法或由相关数据保护机构发布的指导，其效果与上述(i)或(ii)中描述的法律变化相当。
8. *附录的适用范围*。附录 2 所附的标准合同条款和附录 3 的附录仅在适用的数据保护法要求的范围内适用。双方同意遵守此类条款和附录，但这些条款和附录必须符合各司法管辖区适用的数据保护法的要求。
9. *通知*。根据本 DSA 发出的通知（单独称为“通知”）均应采用书面形式。根据本 DSA 发出的通知应按照适用协议的通知条款发出，并将副本通过电子邮件发送给公司 [msd\_privacy\_office@msd.com](mailto:msd_privacy_office@msd.com)，主题行标明“供应商发出的 DSA 通知”，或在发生个人数据泄露的情况下标明“紧急”：个人数据泄露通知”。

**附录 1 – 信息技术安全措施**

1. 定义 - 在本附件中使用时，以下每个定义术语将具有为该术语给出的定义。在本附件中使用但未在此定义的定义术语应具有协议其他部分规定的含义。
   1. “公司信息”指供应商或供应商的任何第三方服务提供商在提供任何服务以及根据协议应被视为机密的任何其他信息中提供、获取、创建或生成或以其他方式处理的公司或公司的任何关联公司或其各自的供应商、客户或其他业务伙伴的任何信息。
   2. “数据泄露”指对任何公司信息的意外或未经授权的破坏、丢失、更改、使用、传输或披露或访问。
   3. “端点”指供应商系统上的任何计算机，包括任何笔记本电脑或台式电脑、移动设备、实验室设备、服务器或其他设备，包括任何托管在外部第三方网站（例如，云提供商）的设备。
   4. “通知事件”指根据任何法律需要通知个人或实体的任何事件，包括数据泄露。
   5. “安全事件”指任何A)数据泄露，(B)通知事件，(C)未经授权的访问或干扰供应商系统的操作或(D)违反供应商在本附件、协议或任何法律下的安全义务。
   6. “主题软件”指提供或用于提供任何服务的任何软件，包括任何交付给或安装在任何计算机，包括任何笔记本电脑或台式电脑、移动设备、实验室设备、服务器、其他设备或公司或公司任何关联公司的信息系统的其他组件上的任何软件。
   7. “供应商系统”指供应商的网络和所有系统，包括主题软件，(A)提供或用于提供任何服务，(B)存储或以其他方式处理或从中访问任何公司信息或公司或其关联公司的交付物或工作进度的任何系统，(C)连接到公司或其关联公司的信息、网络或其他系统或从中访问公司或其关联公司的信息、网络或其他系统的任何系统，或(D)连接到任何上述内容或从中访问任何上述内容的任何系统。
2. 网络安全 - 供应商应维护网络安全政策、程序和控制，并执行与供应商行业最佳实践一致的网络安全活动，但至少包括网络防火墙配置、入侵检测和预防控制、分布式拒绝服务攻击（DDoS）保护控制以及按照供应商行业最佳实践（但不少于每年一次）定期进行的漏洞评估和渗透测试。在任何情况下，供应商应用于保护公司信息和供应商系统的网络安全政策、程序或控制都不应低于供应商应用于保护其自身信息和其他类似性质系统的那些。
3. 应用安全 - 根据所提供服务的性质，如适用，供应商应拥有软件开发生命周期流程和控制（“SDLC流程”），以管理对任何供应商软件的开发和更改，包括更新，升级，补丁，增强，错误修复，修改，改进，修正，修订，发布和其他更改。SDLC流程应至少包括公认的和可比较的行业标准的安全软件开发实践。供应商应遵循一个补丁管理流程，确保供应商信息系统与适当的安全性和功能保持同步。供应商应及时，与风险相称，并在供应商政策和程序中提供的时间范围内，修复和重新测试任何已识别的漏洞。
4. 数据安全 - 根据所提供服务的性质，如适用，供应商应按照公认的和可比较的行业实践和标准处理，存储和以其他方式处理公司信息，例如第11段中规定的（包括适用的PCI DSS）并且应遵守所有法律。供应商应建立并维护防止数据泄露的合理保护措施。除此之外，且不限于供应商的其他义务，供应商应按照供应商行业的最佳实践存储所有公司信息，并遵守所有法律，并应使用符合供应商行业最佳实践的安全措施，包括加密和防火墙，以保护公司信息免受数据泄露。当供应商在离线设施中存储公司信息时，供应商必须遵守协议中的所有条款，或与协议有关的任何协议中的所有条款，这些条款与向第三方披露公司信息或以其他方式聘请第三方提供或协助提供产品或服务有关，供应商应使用公司可以接受的离线存储设施，该设施应完全符合本附件的所有规定。此外，该离线存储设施的提供者必须受到供应商与该提供者之间的书面保密协议的约束，该协议的条款不得比协议或与协议有关的任何协议的条款宽松，并且保护所有存储在其中的公司信息。
5. 数据存储 - 根据所提供服务的性质，如适用，所有公司信息将仅在指定的供应商计算和存储资源上处理，存储和以其他方式处理。公司信息只能在笔记本电脑或移动设备上处理，存储或以其他方式处理或转移到笔记本电脑或移动设备上，如果（A）它是供应商的笔记本电脑或移动设备，（B）供应商按照下文第7段的加密标准对该笔记本电脑或移动设备上的所有公司信息进行加密，并且（C）该笔记本电脑或移动设备受到与公认的和可比较的行业实践和标准一致的端点控制，例如第11段中规定的。公司信息不会在便携式设备上处理，存储或以其他方式处理，除非在上述句子中提供。供应商应将所有公司信息的备份存储为其指定的备份和恢复流程的一部分，这些公司信息的备份必须按照本附件进行加密，包括本第5段和下文第7段的要求。
6. 数据传输 - 根据所提供服务的性质，如适用，任何公司信息的电子传输或交换应通过安全的方式（使用HTTPS或SFTP或等效方式）进行，这些方式符合公认的和可比的行业实践和标准，例如第11段中所述，并且仅根据下文第7段进行。
7. 数据加密 - 根据所提供服务的性质，如适用，除了并不限制供应商的任何其他义务外，供应商同意任何由个人信息组成的公司信息，这些个人信息根据任何法律或由当前支付卡行业数据保护标准保护的信息组成，包括所有公司备份数据，应以加密形式保存，使用商业支持的加密解决方案。供应商同意部署加密解决方案，以符合公认的和可比的行业实践和标准对公司信息进行加密，例如第11段中所述，但对称加密的密钥不少于128位，非对称加密的密钥长度为2048（或更大）位。
8. 数据重复使用 - 根据所提供服务的性质，如适用，供应商应仅为执行服务的目的使用所有公司信息。供应商不得分发，重新定位或在供应商的其他应用程序，环境或业务单位中分享任何公司信息。
9. 协议结束后的数据处理 - 根据所提供服务的性质，如适用，除了并不限制供应商的任何其他义务外，根据公司的要求，除非协议另有规定，协议到期或提前终止后，供应商或供应商的任何关联公司，分包商，服务提供商，代理或其他顾问拥有或控制的所有公司信息应被销毁或退还，由公司选择。
10. 安全漏洞通知 - 除了并不限制供应商的任何其他义务外，供应商应在了解到实际或合理怀疑的安全事件后的24小时内通知公司。供应商应通过电话（+1-704-345-6700 - 选择选项1）和电子邮件Global Operations Center [globalopscnt@merck.com](mailto:globalopscnt@merck.com)联系公司的安全团队，通知公司此类实际或合理怀疑的安全事件。供应商将提供公司可能合理要求的关于安全事件的信息和帮助，包括根源信息。
11. 行业标准 - 通常公认的行业标准包括但不限于以下机构设定和维护的当前标准和基准：
    1. 互联网安全中心 - 参见[http://www.cisecurity.org](http://www.cisecurity.org/)
    2. 支付卡行业/数据安全标准（PCI/DSS）- 参见<http://www.pcisecuritystandards.org/>
    3. 国家标准和技术研究院 - 参见[http://csrc.nist.gov](http://csrc.nist.gov/)
    4. 联邦信息安全管理法（FISMA）- 参见[http://csrc.nist.gov](http://csrc.nist.gov/)
    5. ISO/IEC 27000系列 - 参见<http://www.iso27001security.com/>
    6. 结构化信息标准推进组织（OASIS）- 参见<http://www.oasis-open.org/>
    7. 开放网络应用安全项目（OWASP）- 参见[http://www.owasp.org](http://www.owasp.org/)
    8. CWE（公共弱点枚举）- 请参阅 [http://cwe.mitre.org](http://cwe.mitre.org/) 或 CWE/SANS 顶级 25 编程错误 - <http://cwe.mitre.org/top25/>
    9. SANS研究所- 请参阅 [http://www.sans.org](http://www.sans.org/)
    10. 最危险的软件错误 <http://www.sans.org/top25-programming-errors/>
12. 在公司合理的要求下，供应商应允许公司审计供应商对上述要求的遵守情况。供应商应尽可能快地纠正任何不符合要求的情况。

**附录 2**

如果供应商以标准合同条款第 1 模块要求的方式出口个人信息，则适用以下条款：

*2021 年 6 月 4 日欧盟委员会第 (EU) 2021/914 号实施决定所附标的准合同条款模块 4*  
*（控制者到控制者）正文通过引用并入本文。可选内容如下所述：*

1. *省略第 7 条（对接条款）。*
2. *关于第 11 条，省略了可选文本。*
3. *关于第 17 条，选择选项 1，成员国为荷兰。*
4. *关于第 18 条，选择的管辖地为荷兰。*

**附录 2 的附件 1**

**A. 当事方名单**

*参见协议*

**B. 传输说明**

*参见本协议附件“数据处理详细信息”。*

**C. 主管监督机构**

**法国国家信息与自由委员会 - CNIL**  
3 Place de Fontenoy

TSA 80715

75334 PARIS CEDEX 07  
Tel. +33 1 53 73 22 22  
Fax +33 1 53 73 22 00  
Website: [**http://www.cnil.fr/**](http://www.cnil.fr/)

**附录 2 的附件 2 – 技术和组织措施**

参见附有这些条款的 DSA 附录 1。此外，数据导入者应确保在适当的情况下对所有个人数据  
进行匿名化和加密。此外，当收到政府机构提出的与这些条款所涉及的个人数据相关的请求时，数据导入者及其关联方保证 (i) 美国或其他地方的情报部门或类似机构的访问要求，以及   
(ii) 附件 1B 中所述个人数据的任何“披露义务”，将在提取之前由数据导入者及其关联方根据适用的法律法规和法规提出抗辩。

**附录 3**

**其他州、国家、地区和省的法律要求**

**英国附录：2018 年数据保护法案**

本附录 3 通过引用纳入 2022 年 3 月 21 日生效的《欧盟标准合同条款的国际数据传输附录》  
（B1.0 版），并应视为本协议所有各方已全部签署，涵盖本 DSA 下的所有适用的数据传输，  
包括所有第 2 部分强制性条款。

**瑞士附录：FADP**

1. 就附录 2 中所述数据传输受 FADP 约束而言，对 GDPR 的引用应理解为对《瑞士联邦数据保护法》(“FADP”) 的引用。
2. 在 FADP 规定的期限内，法人实体的个人数据应根据本条款受到与作为数据主体的个人相同的保护。
3. 第 13 条：平行监管
   1. 如果数据传输受 FADP 管辖：联邦数据保护和信息专员 (“FDPIC”) 是主管监督机构；
   2. 如果数据传输受 GDPR 管辖：则第 13(a) 条的标准适用。
4. 第 18(c) 条：选择法院和司法管辖区：惯常居住地在瑞士的数据主体也可以向瑞士法院对数据出口者和/或数据进口者提起法律诉讼。

**加拿大附录：魁北克法 25**

* + - 1. 如果需要收集与本 DSA 条款相关的同意，供应商还必须在协议结束后三 (3) 年内保留所有同意的证据。

**阿联酋附加条款：2021年第45号联邦个人数据保护法**

1. 只要附录2中描述的数据传输受到阿联酋第45号联邦个人数据保护法（“PDPL”）的约束，除非且直到阿联酋数据办公室发布自己的标准合同条款以合法化将个人信息传输到阿联酋之外，并且双方已签订此类标准合同条款，双方同意附录2中所附的标准合同条款应根据具体情况进行适用，以便为个人信息和数据主体提供适当的保障。为此目的： a. 对“欧盟（EU）2016/679条例”、“2016年4月27日欧洲议会和理事会关于自然人数据处理的条例（EU）2016/679（通用数据保护条例）”以及“该条例”的提及，均替换为“PDPL”。 b. 对“欧盟（EU）2016/679条例”特定条款的提及，替换为PDPL的相应条款或章节。 c. 对“欧盟”、“联盟”、“欧盟成员国”、“成员国”及“欧盟或成员国”的提及，均替换为“阿联酋”。 d. 对“主管监督机构”和“监督机构”的提及，均替换为“数据办公室”。 e. 任何因标准合同条款引起的争议，应由阿联酋法律管辖并由阿联酋法院解决。双方同意服从这些法院的管辖。 f. 如果附录2中所附的标准合同条款与PDPL之间存在任何不一致或冲突，以PDPL为准。 g. 如果附录2中所附的标准合同条款在适用于阿联酋之外的个人信息传输方面的含义不明确，或有多个含义，则适用最符合PDPL的含义。
2. 如果阿联酋数据办公室发布了自己的标准合同条款以合法化将个人信息传输到阿联酋之外，双方应本着诚意进行谈判，以期尽快达成并实施标准合同条款。如果双方根据前述句子的规定签订标准合同条款，则此类标准合同条款将取代附录2中所附的标准合同条款，作为在PDPL约束下向阿联酋以外传输个人信息的适当保障措施。
3. 如果数据办公室作出涵盖标准合同条款适用的个人信息传输的充分性决定，或公司另行确定在传输方面适用其他适当的保障措施，公司可通过书面通知供应商撤销其同意受附录2中所附的标准合同条款的约束。自公司根据前述句子发出任何通知之日起，附录2中所附的标准合同条款将不再适用于受PDPL约束的阿联酋之外的个人信息传输。

**巴西附录：LGPD - 标准合同条款**

根据《通用数据保护法》（Lei Geral de Proteção de Dados – “LGPD”）的巴西标准合同条款（“SCCs”）在处理巴西居民数据或任何数据传输需要其应用时必须遵守。各方同意完全采纳由巴西国家数据保护局（“ANPD”）发布的SCCs，除非根据条款明确允许的条款进行修改。此类SCCs通过引用并入协议，当提供多个文本选项时选择如下：

第3.1节选择选项B。进口方可以根据下述情况和第18条规定，执行受这些条款管辖的国际数据传输的个人数据的转移。

第4.1节选择选项A。在不影响相互协助义务和各方的一般义务的前提下，以下指定方应主要负责遵守这些条款中规定的以下义务：

a) 负责发布第14条规定的文件：

[x] 出口方 [ ] 进口方

b) 负责响应第15条中涉及的数据主体请求：

[x] 出口方 [ ] 进口方

c) 负责通知第16条中规定的安全事件：

[x] 出口方 [ ] 进口方

**沙特阿拉伯附录：PDPL - 标准合同条款**

根据《个人数据保护法》（“PDPL”）的沙特阿拉伯标准合同条款（“SCCs”），在处理沙特居民数据、数据传输受沙特管辖或沙特法律要求遵守沙特SCCs时，适用这些条款。与附件2中描述的模板类型一致的SCCs版本完全适用，并通过引用并入协议。