2021 年 11 月 3 日批准

# 约束性企业规则



发布时间：[2021 年 11 月 3 日]
上次审核时间：[2021 年 11 月 3 日]
上次修改日期：[2021 年 11 月 3 日]

## A. 引言

Otis 尊重其所处理个人信息主体的合法隐私权益，如公司董事、主管、员工、承包商、客户、供应商和销售商。

Otis 在处理个人信息时采用《约束性企业规则》（以下简称“BCR”）。Otis Elevator Worldwide BVBA[1] 为“Otis 主管实体”，与 Otis 公司办公室（美国总部）一同负责纠正违反 BCR 的行为。

附录 A 提供了 BCR 中出现的术语和首字母缩略词的定义。

Otis 通常会处理以下三类人群的个人信息：

(1.) 员工：这一类别构成了 Otis 处理的绝大部分的个人信息，包括在此类情况下常见的个人信息（*例如*，身份和联系方式、工资和薪酬、职位、教育背景、健康和安全、培训和评估等）。

(2.) 企业客户和供应商/销售商：Otis 主要将产品和服务销售给企业客户。客户的个人信息主要包括业务联系方式。

(3.) 个人最终用户客户：Otis 的直接个人客户数量有限。

Otis 传输包括人力资源信息（员工和租赁劳动力）在内的个人信息；企业客户、供应商、销售商、销售代表以及其他业务合作伙伴的业务联系方式；Otis 产品消费者的信息，通常是保修信息和有限的信息，如与运营业务部门签订有服务合同的消费者的姓名和地址；访客和非员工销售代表和经销商的信息；以及当用户在使用 Otis 产品和服务时收集的信息。根据提供的产品和服务以及具体服务或项目所需的支持，Otis 会在公司内部传输个人信息。大部分个人信息都传输到位于美国的 Otis 公司办公室。

附录 D 提供了关于 Otis 处理的个人信息的其他信息。

## B. 适用性

**1.** Otis 公司办公室以及执行“集团间协议”的运营业务部门必须遵守上述 BCR。上述实体应确保其员工在处理个人信息时遵守相关 BCR。Otis 将在整个企业建立清晰一致的管控措施，以确保全员遵守 BCR。

[1] 58, Avenue des Arts, 1000 Brussels, Belgium.

**2.** Otis 将遵守全球适用的所有与个人信息保护相关的法律法规。当地法律、法规以及适用于 Otis 的其他限制，如推行的数据保护级别比 BCR 更高，则应以相关法律法规或限制为准。

如果适用法律与 BCR 冲突，可能会妨碍 Otis 公司办公室或一个或多个运营业务部门履行其在 BCR 中规定的义务，或对 BCR 中提供的保证有重大不利影响，则相关实体应立即直接通知 Otis 主管实体和数据隐私全球总监（“隐私主管”），除非执法机构或法律禁止提供此类信息。Otis 隐私主管应协同 Otis 主管实体的 Otis 隐私委员会成员和相关业务部门，共同商议合适的行动方针。对于直接或间接源自欧洲经济区（“EEA”）的个人信息，Otis 应在冲突可能对 BCR 提供的担保产生重大不利影响时随时上报给主管监督机构。

这包括报告第三国执法机构或国家/地区安全机构提出的任何具有法律约束力的个人信息披露请求。此类情况下，Otis 将告知主管监督机构请求的相关情况，包括有关所请求数据的信息、请求机构和披露的法律依据（除非另有禁止，如刑法禁止为执法调查保密）。如果执法机构或法律禁止提供此类信息，则 Otis 应尽最大努力解除禁令，以便遵循本段中所述的程序。任何情况下，如果 Otis 无法免除禁令以便遵循该程序，Otis 将每年向主管监督机构提供一般信息，如请求的次数、所请求的数据类型，以及在可能的情况下，发出请求的政府机构。任何情况下，Otis 不得超出民主社会必要范围，大规模、不成比例、不加辨别地将直接或间接从 EEA 获取到的个人信息传输给任何公共机构。

**3.** 当运营业务部门和公司办公室代表其他 Otis 实体（*即*作为“处理方”）处理个人信息时，也应遵守上述 BCR。负责处理的实体必须受到 BCR 附录 B 中规定的内部处理条款的约束。

**4.** 如果 BCR 与《Otis 公司政策手册》第 24 节之规定有冲突，则在处理直接或间接来自 EEA 的个人信息时应以 BCR 为准。

## C. 范围

虽然 BCR 管理 Otis 对世界各地主体个人信息的处理，但以下 BCR 规定应仅适用于直接或间接来自 EEA 的个人信息：

(1.) 第 B.2 节，关于第三方国家/地区的执法机构或其他政府机构要求披露个人信息；

(2.) 第 B.4 节，关于 BCR 和《公司政策手册》第 24 节规定之间的分歧；

(3.) 第 D.1(a) 节，关于在处理敏感个人信息之前需要获得主体的明确同意；

(4.) 第 D.1(c) 节最后一段，关于保持透明。

(5.) 第 D.1(d) 节对隐私权的要求；

(6.) 第 D.1(e) 节第 2 段，关于违反安全通知的第 (1) 点；

(7.) 第 D.1(f) 节，关于向 EEA 以外的第三方或服务提供商传输个人信息；

(8.) 第 D.5 节最后一段，关于如何提出投诉；以及

(9.) 第 D.6 节第 1 至第 5 段，关于个人和担保的执行权利（第三方受益权）。如 BCR 第 D.6 节最后一段所述，EEA 以外的国家/地区的个人将 BCR 视为传输个人信息的合法手段，因此也应享有第三方受益权。

对于直接或间接从 EEA 获取的个人信息时，则应根据 GDPR 的规定来解释第 D.1 节中所述的隐私原则及其任何部分废除。BCR 中凡有引用 GDPR 之处，都可公开访问以欧盟所有官方语言提供的副本：**https://eur-lex.europa.eu/eli/reg/2016/679/oj**。在 BCR 中引用 GDPR 中的具体条款应视为与 GDPR 规定的相同方式采用相应条款中的原则，即使当个人信息传输到 BCR 所列 EEA 之外的国家/地区时，并不总是遵循 GDPR。

可在附录 C 中查看受 BCR 约束的运营业务部门。

## D. 政策

**1. 隐私原则：**Otis 应在开展所有活动中遵守以下原则：

a) *公平合法地处理个人信息*

只能出于特定的合法目的处理个人信息：(1) 以征得同意为基础；(2) 当原产地法律要求或允许时；或 (3) 出于合法的商业目的，相关个人的利益或基本权利和自由不容忽视，例如大多数人力资源管理、与客户和供应商的业务往来，或存在人身伤害的威胁。

只有在以下情况下，才能处理敏感的个人信息：(1) 数据来源地的法律要求；(2) 在法律允许的情况下，征得个人的明确同意；或 (3) 为保护在身体上或法律上没有能力给予同意的个人的重大利益所必需；或 (4) 公司办公室或运营业务部门建立、行使或维护法律主张。

不得出于任何有背于上述之外的目的进一步处理个人信息，除非：(1) 数据来源地的法律要求；(2) 经个人明确同意（但仅在可以获得同意的情况下）；或 (3) 符合 GDPR 第 6.4 条规定的其他情况。为便于引用，BCR 附录 E 提供 GDPR 第 6.4 条规定的全文。

b) *仅处理相关的个人信息*

Otis 应当采用合适、相关的方式来处理个人信息，并且不能超出处理信息的目的。此外，Otis 不会将个人信息保留超过收集目的所需的时间，除非主体同意用于新的目的或来源地适用的法律、法规、法院诉讼、行政诉讼、仲裁程序或审计规定另有要求。Otis 将会有控制地处理个人信息，旨在确保此类个人信息准确并且处于最新状态。

c) *事先告知个人哪些运营业务部门会处理他们的个人信息*

除非个人已经知道此类信息，否则公司办公事和/或相关运营业务部门在收集个人信息时，应将以下信息告知个人：

- 负责处理个人信息的 Otis 实体（也就是控制方）的身份和联系方式，以及在适用情况下，控制方代表和/或数据保护官的身份和联系方式（联系方式可以是电子邮件联系方式）；
- 待处理个人信息的类别（除非个人已知晓）以及信息来源（除非个人已知晓）；
- 处理或收集个人信息的目的，以及处理的法律依据：
    - 如果法律依据是合法利益，则通知中必须具体说明相关利益；
    - 如果法律依据是法律义务或合同要求，则通知中必须说明个人是否有义务提供个人信息，以及如果个人选择不提供数据可能产生的后果；
    - 如果合法依据是同意，则个人有权随时撤销同意，不会影响撤销前以同意为依据的处理的合法性，以及关于撤销的影响的信息；
- 将与其共享个人信息的接收方或接收方类别；

- 是否会跨境共享个人信息，如果会，是否会将个人信息发送到缺乏充分决定、对适当或合适安全措施的参考，以及获取个人信息副本或已经可以获取到个人信息副本的国家或地区；
- 数据将会保留多久；
- 个人要求访问、纠正、删除和限制处理的权利，以及反对、数据可携带权，向监管机构投诉的权利（针对受 GDPR 管辖的个人和个人信息）；以及
- 如果个人信息受制于自动决定，逻辑、可能的后果和寻求补救的方法。

所有运营业务部门在提供通知时应遵守 GDPR 第 12 条和第 13 条的规定，以 GDPR 的适用范围为限。

如果运营业务部门间接获得个人信息，它们将根据 GDPR 第 14(3) 条通知个人（如上所述），除非个人已经收到通知，或者适用 GDPR 第 14(5) 条规定之外的其他情况。

为便于引用，BCR 附录 E 提供 GDPR 第 13 条和第 14 条规定的全文。

d) *尊重个人对其个人信息行使隐私权的合法权利*

Otis 应允许个人请求访问和更正其个人信息。公司办公室和/或相关运营业务部门将遵守请求，前提是此类请求并非明显毫无根据或实属过分，且无论如何应在收到请求的一个月内处理，不得无故拖延。考虑到请求的复杂程度和数量，必要时这一期限可再延长两个月。公司办公室和/或相关运营业务部门将在收到请求的一个月内通知个人任何此类延期、延期的原因，以及任何拒绝遵守请求和拒绝的原因。公司办公室和/或相关运营业务部门应承担举证责任，证明请求明显没有根据或实属过分。个人可能需要提供身份证明，并可能需要支付 GDPR 允许收取的服务费用。

个人可以反对处理其个人信息，或要求限制处理或删除其个人信息。Otis 将遵守此类请求，除非法规或法律义务要求处理个人信息，以保护公司免受法律索赔，或基于超越个人利益和权利的令人信服的合法理由，如公司审计。个人将被告知因其选择让 Otis 不处理其个人信息而可能产生的后果，例如 Otis 无法提供就业、所请求的服务或进行交易。还会告知个人其请求的后果，并提醒其有权根据 BCR 第 D.5(c) 节之规定提交投诉。

个人有权随时反对出于营销目的处理个人信息。将为不希望接收营销通信的个人提供可轻松访问的方式来反对进一步推送广告，例如，在其账户设置中，或按照电子邮件或通信中链接提供的指示进行操作。如果对于如何应用反垃圾邮件规定有任何疑问，请联系 **privacy@otis.com**。

个人有权不遵守仅基于自动处理（包括特征分析）的决定。如果 Otis 根据个人信息对个人做出自动决定，则 Otis 应提供适当措施来保护个人的合法权益，例如，提供决定背后的逻辑，以及通过人工干预对决定进行审查的机会，并允许个人提出自己的观点并对决定提出异议。

e) *实施适当的技术和组织安全措施*

Otis 应考虑相关处理的敏感性和风险、相关个人信息的性质，以及适用的公司政策，采取适当的安全措施。此类安全措施可酌情包括假名化和加密、确保处理系统的保密性、完整性、可用性和恢复能力的流程、合理保证可用性和可访问性的足够备份，以及对现有安全措施进行定期审计和测试。

运营业务部门应实施健全的数据泄露事件响应计划或遵守 Otis 的数据泄露事件响应计划，这些计划应适当地响应和修正任何实际发生的数据泄露。

数据泄露事件响应计划应至少要求运营业务部门做到：

(1.) 通知 Otis 主管实体和任何其他相关内部隐私职能部门，不得无故拖延，并根据 GDPR 第 33 或 34 条规定，在 72 小时内通知监管机构和/或受影响的个人，不得无故拖延；

(2.) 遵循适当的调查流程，包括记录事件、调查和补救措施；以及

(3.) 根据要求向监管机构提供事件记录。运营业务部门应遵循数据泄露事件响应计划。

Otis 将签订一份书面协议，要求任何内部或外部服务提供商尊重 BCR 或同等规定，并且仅按照 Otis 的指示处理个人信息。书面协议必须使用 Otis 提供的标准条款和条件，如有任何修改必须经过指定的业务部门隐私专业人员或 Otis 隐私主管的批准。涉及受 GDPR 管辖的个人信息服务的协议，应符合 GDPR 第 28 条的规定，标准条款和条件应包括符合第 28 条规定的模板。为便于引用，BCR 附录 E 提供 GDPR 第 28 条规定的全文。

f) *如果没有采取适当的保护措施，不得将个人信息传输给 EEA 以外的第三方或服务提供商*

只有在第三方或服务提供商符合以下条件时，Otis 才能将个人信息传输给它们：(1) 位于提供足够保护级别的国家/地区（定义请参见 GDPR 第 45 条）；(2) 具有满足 GDPR 第 46 条规定的欧盟充足性要求的其他安排；或 (3) 完全遵守 GDPR 第 49 条中列出的减损条款（例外条款）之一，即所有条款均符合 GDPR 第 48 条之规定。为便于引用，BCR 附录 E 提供 GDPR 第 46、48 条和第 49 条规定的全文。在任何情况下，在向服务提供商传输个人数据时，Otis 都应确保在合同中包含第 D.1.e 节中所述的适当条款。

g) *采取适当的问责措施*

作为控制方的每个运营业务部门都应负责并能够证明遵守 BCR。运营业务部门应遵守问责制规定，例如，保存处理操作记录（在处理直接或间接来自 EEA 的个人信息时，应具备 GDPR 第 30 (1) 条中列出的各种要素），根据 GDPR 的规定评估数据保护影响，以及实施适当的技术和组织措施以满足设计隐私和默认隐私的原则。任何涉及 EEA 个人信息的个人信息数据清单都应根据要求提供给主管监督机构。为便于引用，BCR 附录 E 提供 GDPR 第 30 条规定的全文。对于根据 GDPR 第 35 条完成的任何数据保护影响评估，如表明处理将导致高风险且无法有效缓解，则 Otis 应确保根据 GDPR 第 36 条征求主管监督机构的意见。

**2.** **治理：**Otis 致力于维护能够确保符合 BCR 的治理基础设施。此基础设施包括：

a) *道德与合规官*：这一岗位负责促进遵守 BCR，是负责处理与 BCR 有关的内部意见和投诉的内部联系人。Otis 将确保对其道德与合规官进行培训，教授他们如何接收和调查隐私投诉，协助解决隐私问题，并将投诉转发给适当的资源，如适当的隐私专业人员或隐私办公室，以在需要时进行审查和解决。

b) *隐私专业人员*：每个业务部门将任命至少一名隐私专业人员，作为道德与合规官以及业务部门中其他有隐私相关问题的人员的资源。隐私专业人员协助管理层确保本地员工遵守 BCR，并识别和补救业务部门内的不足之处。Otis 将确保这些隐私专业人员拥有足够的资源和独立权限来履行其职责。

c) *数据保护官（以下简称"DPO"）*：DPO 的角色由适用法律定义。当适用法律要求时，会指定 DPO。DPO 会定期配合 Otis 隐私主管的工作。

d) *Otis 隐私委员会（以下简称"OPC"）*：OPC 将负责从总体上监督 Otis 隐私合规计划，包括监督 BCR 的实施情况。OPC 将包括代表各自业务部门的隐私专业人员，以及来自人力资源（"HR"）、信息技术（"IT"）、国际贸易合规（"ITC"）、环境、健康与安全（"EH&S"）、财务、供应管理和 Otis 主管实体的代表。根据需要，可以临时或永久另行增加成员。OPC 与 Otis 隐私主管和隐私办公室合作，制定并确保在全球范围内实施合规性计划，以处理审计团队的调查结果。

e) *全球数据隐私主管（隐私主管）*：隐私主管将与隐私专业人员合作，部署 BCR 并确保有效、高效地实施 BCR。隐私主管还将负责关于数据隐私的培训和意识宣传活动，支持隐私专业人员并确保他们接受培训，同时宣传数据隐私要求的存在和目的，以及保护专有信息的基本要求。隐私主管将指导并领导 Otis 隐私委员会开展工作。隐私主管将作为公司办公室的隐私专业人员，可接触并向最高管理层（*即*董事会）报告，并应得到最高管理层的支持。

f) *隐私办公室*：隐私办公室由隐私主管、隐私专业人员、任命的数据保护官，以及运营业务部门或公司办公室任命的任何其他人员组成。隐私办公室参与 OPC 的工作，回复并解决隐私办公室收到的任何意见或投诉，并协助道德与合规官回应并解决提交给道德与合规官团队的任何意见或投诉。

g) *Otis 主管实体*：Otis 主管实体将通过其隐私专业人员或 DPO 参与 OPC 的工作。如果掌握了违反 BCR 的证据，OPC 或隐私主管将通知 Otis 主管实体，并与 Otis 主管实体协调，与公司办公室和/或相关运营业务部门及其隐私专业人员合作实施适当的补救措施。

**3.** **培训**：Otis 将确保以下类别的人员每年接受有关数据隐私（包括 BCR 相关条款）、安全和/或反垃圾邮件法规的培训：

- 道德与合规官；
- 隐私专业人员；
- 永久或定期访问个人信息，并将处理个人信息作为自身一部分职责的人员；以及
- 参与开发用于处理个人信息的工具的人员。

**4.** **监控和审计**：负责监督内部审计计划的 Otis 内部审计副总裁将至少每季度执行一次审计计划，以评估 BCR 的各个方面的合规性，并将跟进运营业务部门，以确保采取纠正措施。Otis 副总裁、内部审计部门，在内部审计人员、隐私主管和运营业务部门的协助下，将确定 BCR 审计计划的合理范围和规律性（必要时包括临时审计），以处理必须遵守 BCR 的系统和流程。

BCR 合规性审计的结果将传达给隐私主管，隐私主管再将结果告知 Otis 副总裁、法律总顾问、Otis 主管实体和 Otis 隐私委员会。Otis 副总裁、法律总顾问和 Otis 内部审计副总裁，将向董事会或董事会的某个委员会（如审计委员会）传达与 BCR 相关的重大审计结果。欧洲经济区的主管监督机构可根据要求获取与 BCR 相关的审计结果。

**5.** **处理权利请求与投诉**：将按以下规定处理个人提出的关于处理其个人信息的请求。如果当地法律要求，可以补充这些联系方式。无论下述程序如何，个人信息直接或间接来自 EEA 的个人有权直接向监管机构和/或主管法院提交投诉。

*a) 内部 - 来自有权访问 Otis 内网的人员*

Otis 直属员工可以向当地的人力资源代表提出请求和投诉。包括员工在内的所有人员都可以联系他们的道德与合规官、投诉举报部门或隐私办公室。可以通过以下方式联系上述资源：

| | |
|---|---|
| 当地人力资源部门 | 使用常规内部渠道联系 |
| 道德与合规官 | 使用常规内部渠道联系：<br>https://connect.otis.com/business_practices/Pages/default.aspx |
| 投诉举报部门 | 使用常规内部渠道联系或通过以下方式举报：**www.otis.com/reportingchannel** |
| 隐私办公室 | **privacy@otis.com** |

提交给当地人力资源部门、道德与合规官或隐私办公室的投诉：此类投诉将由收到投诉的小组（人力资源部门、道德与合规官或隐私办公室）处理。必要时，由适当的隐私专业人员或隐私主管（或指定人员）协助处理。

提交给投诉举报部门的隐私投诉：只要投诉人寻求进一步的回复并同意，此类投诉将被转交给隐私办公室进行回复和解决。

*b) 外部 - 来自所有其他个人*

所有其他个人的请求和投诉可以提交给投诉举报部门或隐私办公室，联系方式如下：

| | |
|---|---|
| 投诉举报部门 | Diane Andrews，全球隐私顾问 |
| 隐私办公室 | **privacy@otis.com** |

只要投诉人寻求进一步的回复并同意，提交给投诉举报部门的隐私投诉将被转交给隐私办公室进行回复和解决。

*c) 投诉回复*

收到投诉的工作组（以下简称“回复方”）负责提供书面回复（除非个人另有要求，否则可以接受电子邮件）。如果需要提供更多信息，无论是为了验证投诉人的身份还是为了了解投诉的性质，回复方都会联系投诉人，以获取适当的额外信息。如果投诉人不回应或无法建立合理的身份验证，回复方可在 1 个月内通知投诉人 Otis 认定投诉已关闭。

如果 Otis 认为投诉是合理的，则将会努力解决问题，并将解决方案告知投诉人。如果投诉人对解决方案不满意，Otis 将提醒投诉人有权向监管机构和/或主管法院提交投诉。

如果认为投诉不合理，回复方必须向投诉人提供书面解释和通知，说明投诉人有权向监管机构和/或主管法院提交投诉。

如果回复方无法达成令投诉人满意的解决方案（如果投诉合理），或提供令投诉人满意的解释（对于投诉不合理），则回复方必须向隐私主管报告相关问题。隐私主管将审查投诉和回复，以确定进一步的行动是否适当。

如果投诉和审计结果暴露出结构性的全球性不足，则隐私主管将通过 OPC 进行解决，以确保与 Otis 主管实体和当地隐私专业人员合作达成全球解决方案。

提供回复的期限不应超过一个月，除非请求/投诉的复杂程度和范围需要更多时间。这种情况下，在通知个人延迟原因后，回复可再延迟两个月。

BCR 的任何规定不得影响个人根据适用的当地法律，向主管监管机构或法院提交与位于 EEA 的运营业务部门违反适用法律相关的投诉的权利。

对于此类违反 BCR 的行为，个人可以采取以下措施：

- 向主管监督机构提出申诉，特别是在个人常居地、工作地点或被指控发生违规行为的地点所在的国家/地区；或者
- 向有管辖权的欧洲经济区法院提起诉讼，可以是控制方或处理方开展业务所在地的法院，或是个人常居地的法院，依个人选择而定。

**6.** **个人和担保的执行权利：**根据“范围”一节（C 节）中所述的限制，个人应享有本节、B、C、D.1、D.5、D.7、D.8 和 D.9 节中明确授予他们的权利（第三方受益权），以及 Otis 主管实体 (Otis Elevator Worldwide BVBA[2]) 在本节中提供的担保。

根据 BCR 规定拥有上述权利的个人，都可以诉诸其适用的国家/地区法律规定的法定补救程序。位于欧洲经济区之外且违反 BCR 的运营业务部门，同意欧洲经济区的法院或其他主管当局对涉嫌违反 BCR 的行为拥有管辖权，并且个人将拥有针对 Otis 主管实体的权利和补救措施，如同相关违规行为是在 Otis 主管实体所在成员国中造成的一样。

在 Otis 公司办公室的协助下，Otis 主管实体应负责确保采取行动 (1) 补救 Otis 公司办公室或位于欧洲经济区以外地区的运营业务部门的违规行为；(2) 向本节提及的个人支付本公司办公室和/或位于欧洲经济区以外地区的运营业务部门违反 BCR 造成的任何重大或非重大损失或罚款的赔偿，除非相关运营业务部门已经补救违规行为或支付赔偿。

[2]注册地址：58, Avenue des Arts, 1000 Brussels, Belgium, and [registration number – 0652.780.207。

如果个人能够证明他们遭受了损失，则 Otis 主管实体应与 Otis 公司办公室一起，证明公司办公室和相关运营业务部门没有违反其在 BCR 中规定的义务。如果能够提供此类证明，则 Otis 主管实体可以不用承担 BCR 规定的任何责任。

对于承认 BCR 是传输个人信息的合法手段的 EEA 成员国之外的国家/地区，这些国家/地区的个人应享有根据 D.1、D.5、D.7 和 D.9 节明确授予他们的权利。因此，这些国家/地区中受影响的个人可以在所在地采取任何行动，强制要求违反 BCR 规定的运营业务部门遵守相关规定。

7. **与监管机构合作：**运营业务部门应根据主管监管机构要求，协助其调查和验证 BCR，包括根据要求提供审计结果。

Otis 应遵守 EEA 主管监管机构的决定，并从 BCR 相关监管机构那里征求建议。Otis 同意主管监管机构可根据 EEA 适用法律，对其对 BCR 的遵守情况开展审计工作。

8. **修改 BCR 规定：**如果对 BCR 进行了任何修改或变更，从而实质性地改变了其中规定的保护级别，Otis 主管实体应立即通知比利时监督机构；Otis 主管实体应每年一次将前一年发生的所有变更通知比利时监督机构，并简要说明变更原因。Otis 还应承诺通过通知 OPC（包括所有隐私专业人员和 DPO，两者应转而通知受约束的运营业务部门），将任何变更通知给所有受约束的运营业务部门，不得无故拖延。

Otis 隐私主管应持有一份最新的清单，列出所有已执行集团间协议的运营业务部门，以及 BCR 的所有更新规定。这份清单应根据要求提供给受约束的运营企业、个人及 EEA 监管机构。任何情况下，Otis 隐私主管或 Otis 主管实体应至少每年一次，向比利时监管机构提供一份最新清单，列出已执行集团间协议的所有运营业务部门。

Otis 同意，在相关集团成员执行集团间协议并遵守该协议之前，Otis 不得以 BCR 为依据，将个人信息传输给 Otis 集团的其他成员。Otis 不得将个人信息传输给向新的 BCR 成员，直到新的 BCR 成员受到 BCR 的有效约束并能够遵守相关规定。如果非 EEA BCR 成员不再是集团的一部分或不再受 BCR 约束，应继续保留在 BCR 约束期间与直接或间接从 EEA 获得的任何个人信息相关的义务，直到相关个人信息被返回、删除、抹去或匿名化。

9. **传达 BCR：**为了确保个人了解他们根据 BCR 享有哪些权利，运营业务部门应在其面向外部的网站上发布或维护 BCR 的链接。Otis 应在 **www.otis.com** 或任何替代网站上发布或维护 BCR 的链接。

# 附录 A - 定义

**“业务部门”**是指 Otis 的主要部门，这些部门可能会不时发生变化，目前等同于北美、拉丁美洲、EMEA、亚太地区、中国和 Otis 公司办公室。

**“同意”**是指个人在不受限制的情况下给出的具体、知情和明确的声明或确认行动，表示自己愿意同意处理与其相关的个人信息。

**“控制方”**是指单独或与他人共同决定个人信息处理目的和方式的自然人或法人、公共机构、代理机构或其他团体。

**“公司办公室”**是指位于美国康涅狄格州法明顿市 One Carrier Place 的公司总部，邮编 06032。

**“数据泄露”**是指导致意外或非法破坏、丢失、更改、未经授权披露或访问传输、存储或以其他方式处理的个人信息的安全漏洞。

**“EMEA”**是指欧洲、中东和非洲地区。

**“GDPR”**是指《欧盟通用数据保护条例》。

**“个人”**是指其个人信息由 Otis 处理的自然人。

**“经营业务部门”**是指 Otis 的业务部门、单位和分部，以及位于任何地区的所有其他经营实体（包括 Otis 拥有控股权或有效管理控制权的受控合资企业、合伙企业和其他业务安排），除了公司办公室。

**“个人信息”**是指与已识别或可识别的自然人相关的任何信息；可识别的自然人是指可以直接或间接识别的人员，特别是通过参考诸如姓名、身份证号码、位置数据、网络标识符等标识符或该自然人的身体、生理、遗传、精神、经济、文化或社会身份所特有的一个或多个因素。

**“人员”**是指 Otis 员工，包括 Otis 董事和主管，以及 Otis 雇佣的临时员工、承包商、租赁劳工和合同工。

**“处理”**（包括其类似形式）是指对个人信息进行的任何操作或一系列操作，无论是否通过自动方式进行，如收集、记录、组织、存储、改编或修改、检索、咨询、使用、通过传输、转移、传播或其他方式披露、调整或组合、阻止、擦除或销毁。

**“敏感的个人信息”**包含在个人信息的范畴之内，此类信息会揭示：种族或民族血统、政治观点、宗教或哲学信仰或工会会员身份；以及处理遗传数据、用于独特识别自然人的生物特征数据、关于健康或个人性取向或性生活的数据；或犯下或被指控犯下任何罪行及可能的惩罚。

**“服务提供商”**或**“处理方”**是指代表 Otis 处理或以其他方式被允许通过直接向 Otis 提供服务来访问由 Otis 处理的个人信息的任何实体或个人。

**“监管机构”**应与 GDPR 中所给出的含义保持一致。

**“Otis”**是指 Otis 的公司办公室及其运营业务部门。

## 附录 B - 内部处理条款

以下条款适用于受 BCR 约束的运营业务部门（以下简称“Otis 委托方”）将涉及所涵盖个人信息处理的项目，委托给另一个受约束的运营业务部门（以下简称“Otis 处理方”）的情况。如果项目涉及 Otis 委托方和 Otis 处理方之间的书面文件（“工作订单”），工作订单应引用以下条款中的内部处理条款：“本工作订单中规定的服务受 Otis BCR 中旨在保护个人信息的内部处理条款管辖。”

这些条款中定义的术语是指 Otis BCR 中定义的术语。

1. Otis 委托方和 Otis 处理方同意在整个工作订单期间遵守 Otis BCR。整个工作订单期间都应遵守相应条款。第 4.2、4.4、4.5、4.8、4.10 和 4.11 节之规定应在工作订单终止后继续生效。

2. 在履行服务时，Otis 处理方将代表 Otis 委托方处理个人信息。

3. Otis 委托方具有以下义务：

   3.1. Otis 委托方应向 Otis 处理方提供明确说明，告知处理相关个人信息的性质、目的和持续时间。说明应做到足够明确，以允许 Otis 处理方履行其在相关条款和 Otis BCR 中规定的义务。特别是，Otis 委托方提供的说明可能管辖对于分包商的使用、披露个人信息，以及 Otis 处理方的其他义务。

   3.2. Otis 委托方应告知 Otis 处理方其国家/地区颁布的数据保护法和相关法律手段、法规、命令，以及与 Otis 处理方根据相应条款进行的处理相关的类似法规的所有修正案，并就 Otis 处理方应如何遵守这些修正案提供说明。

4. Otis 处理方须承担的义务

   4.1. Otis 处理方应根据 Otis 委托方的指示处理个人信息，相关指示记录在工作订单中，并以书面形式传达。Otis 处理方不得出于任何其他目的，或以任何其他方式处理相关个人信息。

   4.2. Otis 处理方应遵守 Otis BCR 的所有规定，尤其是第 D.1.e 节之规定。

   4.3. 根据本条款第 4.6 节规定，未经 Otis 委托方事先书面授权，Otis 处理方不得向子处理方之外的任何第三方披露或传输相关的个人信息。

4.4. 如果根据 Otis BCR（第 D.1.f 节）规定，尽管有第 4 节之规定，Otis 处理方因有效的法律义务规定其执行处理，则仍应实施处理。这种情况下，Otis 处理方应在遵守任何此类规定之前书面通知 Otis 委托方（除非适用的法律、法规或政府机构禁止提供此类通知），并应遵守 Otis 委托方关于此类披露提供的所有合理指示。

4.5. 当相关个人行使与其个人信息相关的权利时，Otis 处理方应在收到来自任何个人的任何通信后的三 (3) 个工作日内通知 Otis 委托方，并应遵守 Otis 委托方在回复此类通信时提供的所有指示。此外，Otis 处理方应提供 Otis 委托方要求的任何协助，以回复任何个人发送的通信，说明他/她在其个人信息方面享有的权力。

4.6. Otis 处理方可雇用子处理方协助其履行工作订单中规定的义务，前提是其已获得 Otis 委托方事先书面批准。Otis 处理方将与任何子处理方签订书面协议，其中规定子处理方须承担的义务不亚于 Otis 处理方在这些条款中规定的义务。Otis 处理方必须遵守 Otis BCR 第 D.1.f 节之规定

4.7. Otis 处理方声明并保证，其遵守的任何数据保护立法（或任何其他法律或法规）均不妨碍其履行这些条款规定的义务。如果任何此类法律的变更有可能对 Otis 处理方遵守这些条款产生重大不利影响，或者如果 Otis 处理方不能遵守这些条款，Otis 处理方应在十五 (15) 个工作日内通知 Otis 委托方，而 Otis 委托方应有权立即终止工作订单。

4.8. Otis 处理方同意，Otis 委托方可以要求按照 Otis BCR 第 D.4 节之规定，对 Otis 处理方遵守相应条款的情况进行审计。尤其是，Otis 处理方应向 Otis 委托方提供证明其遵守这些义务的所有必要信息，并提交给审计部门，包括接受由 Otis 委托方或由其委托的审计员实施的检查。

4.9. Otis 处理方应确保任何在其授权下处理个人信息的个人承担适当的保密责任。

4.10. Otis 处理方应协助 Otis 委托方履行其在适用的数据保护法中规定的义务，包括完成数据保护影响评估和征求监管机构意见（如适用）。

4.11. Otis 处理方应及时通知 Otis 发生的数据泄露事件，并应立即采取措施纠正和防止数据泄露事件再次发生，并在需要时协助 Otis 采取同样的措施。Otis 或相应运营业务部门将与 Otis 委托方和 Otis 处理方协商，进行适当的调查和补救。Otis 处理方还应在必要时协助 Otis 委托方，以履行后者向政府机构或受影响的个人通知数据泄露的义务。

4.12. Otis 处理方应根据 Otis BCR 第 D.1.e 节之规定，采取适当的技术和组织措施，以确保其代表 Otis 委托方处理的个人信息的风险在可接受的安全等级之内。

5. 如果工作订单终止，则 Otis 处理方应向 Otis 委托方发送 Otis 处理方持有的所有相关个人信息，连同相关数据在任何媒介中的所有副本，或销毁相关数据，除非任何适用的法律、法规或政府机构要求 Otis 处理方保留相关个人信息或其中一部分。这种情况下，Otis 处理方应立即将此等义务告知 Otis 委托方。

6. 上述条款应受 Otis 委托方所在国家/地区的法律管辖并据其所在地法律进行解释。在不违反 Otis BCR 第 D.6 节的情况下，上述条款的每一方不可撤销地接受 Otis 委托人所在地法院，对上述条款引起的或与上述条款有关的任何索赔或事项具有专属管辖权。

7. 其他

   7.1. 上述条款的规定可以分割。如果任何短语、条款或规定全部或部分无效或不可执行，则此类情况仅影响相应短语、条款或规定，相应条款的其余部分应保持完全有效。

   7.2. 上述条款的规定应符合 Otis 委托方和 Otis 处理方及其各自继承人和转让的权利，并对其具有约束力。

## 附录 C – 受约束实体清单

可应要求提供受约束实体清单，如需请求或希望咨询问题，请发送电子邮件至 **privacy@otis.com**。

## 附录 D

### Otis 处理的个人信息类型说明

下表汇总了 Otis 可能在其业务范围内处理的个人信息的主要类型。下面列出的个人信息类型将根据具体情况进行收集，并且将始终按照法律和当地法规要求收集，包括 BCR 中其他章节所述的敏感个人信息。

| 个人信息的类型 |
| --- |
| **姓名**：姓名，包括名字、姓氏、中间名、任何后缀（如小或老）和称呼（如先生或女士）。 |
| **身份详细信息**：出生日期、性别，以及政府颁发的身份证件（包括护照和签证）；出生地、公民身份和居留身份，所有这些信息均符合适用的法律。 |
| **工作联系方式和雇主详细信息**：包括工作电话号码、传真号码、工作电子邮件地址、邮寄地址和工作地点在内的信息；雇主相关信息，包括公司名称、公司位置、公司地址和注册国家/地区。 |
| **个人联系方式**：家庭住址、个人电子邮件地址和家庭电话号码，包括个人的手机号码。 |
| **紧急联系方式**：个人配偶或近亲的姓名及联系方式等**信息**。 |
| **背景和职业数据**：工作经验、教育和工作经历、技能类别，包括语言技能、执照、证书、从事某项工作的授权书，或者贸易协会或专业组织的成员资格和参与情况；适用规定和法律要求的兵役信息；关于工作偏好的信息，例如出差和位置偏好。 |
| **人力资源和工作相关数据**：员工或承包商的相关信息：职称、部门、工作职责和成本中心（如适用）；主管和/或助理的姓名；可能包括与个人相关的工作任务和工作成果；个人参与的工作协议、计划和活动；支持人力资源应用程序所需的其他数据，包括工资单、差旅和费用管理；培训、发展和/或绩效评估信息；时间收集和分配信息；作为任务一部分而收集的信息，例如时间和出勤、身份信息或用于特定角色或任务的地理位置数据，和/或安全许可数据（所有这些信息均符合适用的法律）；继任计划信息；税务相关信息，如婚姻状况、与投保人的关系和/或家属；有关健康和伤病的信息，如残疾、病假、产假，以及管理人力资源和提供相关福利/服务可能需要的其他信息。 |

| 个人信息的类型 |
| --- |
| **系统访问和 IT 安全数据**：Otis 电脑、网络和通信信息和日志，涵盖公司电话、电脑、电子通信（如电子邮件和电子日历）以及其他信息和通信技术的使用，包括但不限于用户名/登录标识、密码、安全问题的答案，以及访问 Otis 应用程序、网络、系统和服务所需的其他信息，以及个人通过 Otis 网络和系统存储、发送、提交或接收的信息。 |
| **物理安全数据**：与进入 Otis 场所相关的信息，以确保物理安全并防止有人未经授权进入，包括门禁、灾难应急措施和其他必要信息。 |
| **EHS 数据**：确保 Otis 场所的安全，以及遵守环境、健康和安全法规所需的信息，包括在 Otis 场所或工作期间发生的事故记录。 |
| **产品/服务相关数据**：为促进服务或请求帮助而提供的信息，如产品使用或问题信息，包括提供定位服务的某些站点的位置信息；某些产品的遥测信息处理数据；提供产品或服务的付款、发票和财务数据；保修相关信息。 |
| **网站和应用程序数据**：通过使用 Otis 网站或应用程序收集到的信息，例如设备标识符、IP 地址、日志文件和位置数据，所有信息均符合适用的法律。 |
| **其他数据（如适用）**：语言和通信偏好；个人自愿在电子系统的个人资料中填写的信息；事件注册信息；访客数据，包括访问时间、日期和地点，以及批准或拒绝的筛查结果（如适用）；根据适用法律提供或接受的礼物清单；通过自愿调查或促销或通过使用产品收集的信息；国际贸易合规可能需要的其他信息。 |

## Otis 处理的个人信息目的说明

下表汇总了 Otis 可能在其业务范围内出于哪些主要目的而处理个人信息。

| 目的 | 信息被处理的个人 | | | | | |
|---|---|---|---|---|---|---|
| | 员工和外包劳动力（如适用） | 求职者 | 供应商、销售商和业务客户的人员 | Otis 系统和设施的访客 | 获得授权使用 Otis 系统的人员 | Otis 某些产品的消费者和最终用户 |
| 管理招聘，包括：薪酬和福利，包括制定和管理福利计划；工资单管理，如扣款和缴费；职业发展、绩效反馈和进展；奖励和认可；时间收集和分配；差旅和费用报销，包括差旅和/或信用卡管理；培训；异地搬迁、委派函、对外籍雇员的支持、签证、许可证和其他工作权授权；纳税申报和预扣税；维护员工和管理人员的简历和履历；业务规划；电子邮件系统和组织结构图；健康与安全计划、体检；审计与合规审查；管理内部调查。 | 姓名；身份详细信息；工作联系人和雇主详细信息；个人联系方式；紧急联系方式；背景和职业数据；人力资源和工作相关数据；系统访问和 IT 安全数据；物理安全数据；EHS 数据；物理安全数据；网站和应用程序数据；其他数据 | | | | | |

| 目的 | 信息被处理的个人 | | | | | |
|---|---|---|---|---|---|---|
| | 员工和外包劳动力（如适用） | 求职者 | 供应商、销售商和业务客户的人员 | Otis 系统和设施的访客 | 获得授权使用 Otis 系统的人员 | Otis 某些产品的消费者和最终用户 |
| 管理劳工和员工关系，包括申诉程序 | 姓名；身份详细信息；工作联系方式和雇主详细信息；人力资源和工作相关数据；系统访问和 IT 安全数据；EHS 数据；物理安全数据；网站和应用程序数据；其他数据 | | | | | |
| 促进开展投资者管理活动 | 工作联系方式和雇主详细信息；人力资源和工作相关数据 | | | | | |
| 人员配备和人员继任规划，包括可能影响预算和财务规划及报表的事项 | 工作联系方式和雇主详细信息；人力资源和工作相关数据 | | | | | |

| 目的 | 信息被处理的个人 | | | | | |
|---|---|---|---|---|---|---|
| | 员工和外包劳动力（如适用） | 求职者 | 供应商、销售商和业务客户的人员 | Otis 系统和设施的访客 | 获得授权使用 Otis 系统的人员 | Otis 某些产品的消费者和最终用户 |
| 保护知识产权，包括但不限于专利归档 | 工作联系方式和雇主详细信息；系统访问和 IT 安全数据 | | 工作联系方式和雇主详细信息；系统访问和 IT 安全数据 | | | |
| 开展常规业务运营，包括设计和开发产品、管理企业资源规划 (ERP) 系统、发送发票和收款、付款以及向客户提供商品和服务，其中可能包括与客户或其他业务合作伙伴共享有限的个人信息 | 姓名；工作联系方式和雇主详细信息；人力资源和工作相关数据；产品/服务相关数据；网站和应用程序数据；其他数据 | | 姓名；工作联系方式和雇主详细信息；产品/服务相关数据；网站和应用程序数据；其他数据 | 姓名；工作联系方式和雇主详细信息；产品/服务相关数据；网站和应用程序数据；其他数据 | 姓名；工作联系方式和雇主详细信息；产品/服务相关数据；网站和应用程序数据；其他数据 | 姓名；工作联系方式和雇主详细信息；产品/服务相关数据；网站和应用程序数据；其他数据 |
| 提供所请求的信息、产品和服务，其中可能包括某些应用以已知和透明的方式使用地理定位 | 产品/服务相关数据； | | 产品/服务相关数据； | | | 产品/服务相关数据； |
| 开展和管理敬业度调查和慈善活动 | 其他数据 | | | | | 其他数据 |
| 报告和统计分析，包括全球企业员工人数、人口统计和适用法律要求提供的报告 | 工作和雇主详细信息；与工作相关的数据 | | | | | 工作和雇主详细信息 |

| 目的 | 信息被处理的个人 | | | | | |
|---|---|---|---|---|---|---|
| | 员工和外包劳动力（如适用） | 求职者 | 供应商、销售商和业务客户的人员 | Otis 系统和设施的访客 | 获得授权使用 Otis 系统的人员 | Otis 某些产品的消费者和最终用户 |
| 应对涉及健康或安全风险的情况，包括紧急情况 | EHS 数据；物理安全数据 | | EHS 数据；物理安全数据 | EHS 数据；物理安全数据 | EHS 数据；物理安全数据 | EHS 数据；物理安全数据 |
| 管理通信和通知 | 姓名；工作联系方式和雇主详细信息； | | 姓名；工作联系方式和雇主详细信息； | 姓名；工作联系方式和雇主详细信息； | 姓名；工作联系方式和雇主详细信息； | 姓名；工作联系方式和雇主详细信息； |
| 管理物理安全，包括门禁和安全、设施访问权限和安全，以及灾难应急预案 | 姓名；工作联系方式和雇主详细信息；系统访问和 IT 安全数据；EHS 数据；物理安全数据；其他数据 | | 姓名；工作联系方式和雇主详细信息；EHS 数据；物理安全数据；其他数据 | 姓名；工作联系方式和雇主详细信息；EHS 数据；物理安全数据；其他数据 | 姓名；工作联系方式和雇主详细信息；EHS 数据；物理安全数据；其他数据 | 姓名；工作联系方式和雇主详细信息；EHS 数据；物理安全数据；其他数据 |
| 管理、维护和保护信息技术（“IT”）系统 | 姓名；工作联系方式和雇主详细信息；系统访问和 IT 安全数据 | | 姓名；工作联系方式和雇主详细信息；系统访问和 IT 安全数据 | 姓名；工作联系方式和雇主详细信息；系统访问和 IT 安全数据 | 姓名；工作联系方式和雇主详细信息；系统访问和 IT 安全数据 | 姓名；工作联系方式和雇主详细信息；系统访问和 IT 安全数据 |

| 目的 | 信息被处理的个人 | | | | | |
|---|---|---|---|---|---|---|
| | 员工和外包劳动力（如适用） | 求职者 | 供应商、销售商和业务客户的人员 | Otis 系统和设施的访客 | 获得授权使用 Otis 系统的人员 | Otis 某些产品的消费者和最终用户 |
| 确保遵守进出口和其他国际贸易管制措施，包括管理注册和授权，确定受控技术和/或商品的访问权限，以及筛选受制裁或受限制的国家/地区或相关方 | 姓名；身份详细信息；工作联系方式和雇主详细信息 | | 姓名；身份详细信息；工作联系方式和雇主详细信息 | 姓名；身份详细信息；工作联系方式和雇主详细信息 | 姓名；身份详细信息；工作联系方式和雇主详细信息 | 姓名；身份详细信息；工作联系方式和雇主详细信息 |
| 对索赔进行起诉和辩护，并对执法请求做出回应（如有要求，且仅根据适用法律） | 法律要求提供的或为达到此目的所需的任何类别 | 法律要求提供的或为达到此目的所需的任何类别 | 法律要求提供的或为达到此目的所需的任何类别 | 法律要求提供的或为达到此目的所需的任何类别 | 法律要求提供的或为达到此目的所需的任何类别 | 法律要求提供的或为达到此目的所需的任何类别 |
| 提供客户服务和支持，培训和认证客户、供应商和销售商人员，并进行尽职调查和风险评估 | | | 姓名；工作联系方式和雇主详细信息；其他数据 | 姓名；工作联系方式和雇主详细信息；其他数据 | 姓名；工作联系方式和雇主详细信息；其他数据 | 姓名；工作联系方式和雇主详细信息；其他数据 |
| 与使用 Otis 网站和应用程序相关的目的，包括回复请求或进一步处理提交的表格；宣传与 Otis 相关的产品、服务、促销和活动；改进我们的产品、服务、网站和应用程序；防范欺诈或调查可疑或实际存在的非法活动；开发新产品，提高产品质量，改善和个性化用户体验。 | 姓名；工作联系方式和雇主详细信息；网站和应用程序数据 | 姓名；工作联系方式和雇主详细信息；网站和应用程序数据 | 姓名；工作联系方式和雇主详细信息；网站和应用程序数据 | 姓名；工作联系方式和雇主详细信息；网站和应用程序数据 | 姓名；工作联系方式和雇主详细信息；网站和应用程序数据 | 姓名；工作联系方式和雇主详细信息；网站和应用程序数据 |

| 目的 | 信息被处理的个人 | | | | | |
|---|---|---|---|---|---|---|
| | 员工和外包劳动力（如适用） | 求职者 | 供应商、销售商和业务客户的人员 | Otis 系统和设施的访客 | 获得授权使用 Otis 系统的人员 | Otis 某些产品的消费者和最终用户 |
| 求职目的，包括：接收求职；评估申请；安排和进行电话筛选、面谈和其他适用的评估；就申请或其他机会与申请人联系；交流变化；验证引荐人调查，进行背景调查（根据适用法律适当开展）；筛选；促进招聘；遵守法律和监管要求；验证身份以确保安全；提供反馈机会；并对申请人趋势进行分析，以了解和改进 Otis 的招聘活动。 | | 姓名；身份详细信息；工作联系方式和雇主详细信息；个人联系方式；背景和职业数据；网站和应用程序数据 | | | | |