Approved November 3, 2021

Binding Corporate Rules

Issued: [November 3, 2021]
Last reviewed: [November 3, 2021]
Last revised: [November 3, 2021]

A. INTRODUCTION

Otis respects the legitimate privacy interests of the people from whom it Processes Personal Information, such as its directors, officers, employees, contractors, customers, suppliers, and vendors.

Otis has adopted Binding Corporate Rules ("BCRs") for the Personal Information that it Processes about Individuals. Otis Elevator Worldwide BVBA[1] is the "Otis Lead Entity" and, in coordination with the Otis Corporate Office (the U.S. headquarters), has responsibility for remedying breaches of the BCRs.

Exhibit A provides definitions for terms and acronyms used in these BCRs.

Otis Processes the Personal Information of Individuals who generally fall into the following three categories:

(1.) Employees: This category makes up the vast majority of Personal Information that Otis Processes, including Personal Information that is common in such contexts (*e.g.*, identification and contact information, salary and compensation, position, education, health & safety, training, and evaluation).

(2.) Business customers and suppliers/vendors: Otis sells its products and services mostly to business customers. The Personal Information for customers includes mainly business contact information.

(3.) Individual end-user customers: Otis has a limited number of direct individual customers.

Otis transfers Personal Information including human resources information (employees and leased labor); business contact information for business customers, suppliers, vendors, sales representatives, and other business partners; information from consumers of Otis products, generally warranty information and limited information, such as name and address, on consumers who have a service contract with an Operating Business; information on visitors and non-employee sales representatives and distributors; and information collected on the use of Otis products and services by users of those products and services. Personal Information is transferred within Otis depending on the products and services provided and the support required for particular services or projects. The bulk of Personal Information is transferred to the Otis Corporate Office, located in the U.S.

Exhibit D provides additional information on Personal Information Processed by Otis.

B. APPLICABILITY

1. These BCRs are mandatory for Otis's Corporate Office and the Operating Businesses that have executed the Intra-Group Agreement. These entities shall ensure that their Personnel comply

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

with these BCRs when Processing an Individual's Personal Information. Otis will establish clear and consistent controls across the enterprise to ensure compliance with the BCRs.

2. Otis will comply with all laws and regulations related to the protection of Personal Information applicable to it worldwide. Provisions of local laws, regulations, and other restrictions applicable to Otis that impose a higher level of data protection shall have precedence over the BCRs.

If applicable law conflicts with these BCRs in that it might prevent Otis's Corporate Office or one or more Operating Businesses from fulfilling their obligations under the BCRs or has a substantial adverse effect on the guarantees provided therein, the entity concerned shall promptly and directly notify the Otis Lead Entity and Global Head of Data Privacy ("Privacy Lead"), except where providing such information is prohibited by a law enforcement authority or law. The Otis Privacy Lead, in cooperation with the Otis Privacy Council member for the Otis Lead Entity and the entity and Business Units concerned, shall determine the appropriate course of action. For Personal Information originating directly or indirectly from the European Economic Area ("EEA"), Otis shall report to the competent Supervisory Authority any time that the conflict is likely to have a substantial adverse effect on the guarantees provided by these BCRs.

This includes reporting any legally binding request for disclosure of Personal Information by a law enforcement authority or state security body of a third country. In such a case, Otis will inform the competent Supervisory Authority about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). Where providing such information is prohibited by a law enforcement authority or law, Otis shall make its best effort to have the prohibition waived so that the process otherwise described in this paragraph may be followed. If there are any cases where Otis is unable to have the prohibition waived so that this process may be followed, Otis will provide, on an annual basis, the competent Supervisory Authority with general information, such as the number of requests, the type of data requested, and, where possible, the requesting governmental body. In all instances, any transfer of Personal Information originating directly or indirectly from the EEA by Otis to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

3. These BCRs also apply to Operating Businesses and to the Corporate Office when they Process an Individual's Personal Information on behalf of other Otis entities (*i.e.*, as Processors). The Processing entities must be bound by the Internal Processing Clauses set out in Exhibit B to these BCRs.

4. In case of a conflict between these BCRs and the Otis Corporate Policy Manual, Section 24, these BCRs prevail for Personal Information originating directly or indirectly from the EEA.

C. SCOPE

These BCRs govern the Processing by Otis of Personal Information of Individuals wherever located, except that the following provisions of the BCRs shall only apply to Personal Information originating directly or indirectly from the EEA:

(1.) Section B.2, relating to requests for disclosures of Personal Information by a law enforcement authority or other governmental authority of a third country;

(2.) Section B.4 relating to discrepancies between the BCRs and Corporate Policy Manual, Section 24;

(3.) Section D.1(a) in relation to the requirement to obtain explicit consent for Sensitive Personal Information;

(4.) Section D.1(c), last paragraph on transparency;

(5.) the requirements of D.1(d) on privacy rights;

(6.) Section D.1(e), paragraph 2, point (1) on security breach notification;

(7.) Section D.1(f) relating to transfers of Personal Information to Third Parties or Service Providers outside the EEA;

(8.) the last paragraph of Section D.5 on bringing complaints; and

(9.) Section D.6, paragraphs 1 through 5 regarding the enforcement rights of Individuals and guarantees(third party beneficiary rights). Individuals in countries outside of the EEA that recognize these BCRs as a lawful instrument to transfer Personal Information, shall also have the benefit of third party beneficiary rights, as explained in the last paragraph of Section D.6 of these BCRs.

In relation to Personal Information originating directly or indirectly from the EEA, the privacy principles in Section D.1 and any derogations thereto shall be interpreted in light of the GDPR. Wherever there is a reference to the GDPR in these BCRs, a publicly available copy can be accessed in all languages of the European Union at: **https://eur-lex.europa.eu/eli/reg/2016/679/oj**. In these BCRs, references to specific articles of the GDPR should be understood as applying the principles in those articles in the same way as they would apply under the GDPR, even though the GDPR does not always apply to Personal Information once it is transferred out of the EEA under these BCRs.

The Operating Businesses bound by these BCRs can be found in Exhibit C.

D. POLICY

1. Privacy Principles: In all of its activities, Otis shall:

a) *Process Personal Information fairly and lawfully*

Individuals' Personal Information shall only be Processed for specified and legitimate purposes (1) on the basis of consent; (2) when required or permitted by law in the country

of origin; or (3) for a legitimate business purpose not outweighed by the interests or fundamental rights and freedoms of the Individuals concerned, such as most human resources management, business interactions with customer and supplier, or a threat of physical harm.

Individuals' Sensitive Personal Information shall only be Processed when: (1) required by law in the country of origin of the data; (2) with the explicit consent of the Individual where permitted by law; or (3) when necessary to protect the vital interests of an Individual who is physically or legally incapable of giving consent; or (4) the establishment, exercise, or defense of a legal claim by the Corporate Office or an Operating Business.

Individuals' Personal Information shall not be further Processed for any incompatible purposes unless: (1) required by law in the country of origin of the data; (2) with the explicit consent of the Individual (but only in situations where consent can be obtained); or (3) otherwise in compliance with Art 6.4 GDPR. For ease of reference, Exhibit E of these BCRs provides the full text of Article 6.4 GDPR.

b) *Only Process Personal Information that is relevant*

Otis shall Process Individuals' Personal Information in a manner that is adequate, relevant and not excessive in relation to the purpose(s) for which the information is Processed. In addition, Otis will not keep Individuals' Personal Information for longer than necessary for the purpose(s) for which it was collected, unless with consent when used for a new purpose or otherwise required in the country of origin by applicable law, regulation, court proceedings, administrative proceedings, arbitration proceedings, or audit requirements. Otis will Process Individuals' Personal Information under its control in a manner that is intended to ensure that such Personal Information is accurate and current.

c) *Provide appropriate notice to Individuals whose Personal Information the Operating Businesses Process*

Unless the Individual is already aware of this information, the Corporate Office and/or the relevant Operating Business shall, at the time of collecting Personal Information, provide notice to Individuals of:

- The identity and contact details of the Otis entity that is responsible for the Personal Information (in other words, is the Controller) and, where applicable, of the Controller's representative and/or data protection officer (contact details may be an email contact);

- Categories of Personal Information that will be Processed (unless already known by the Individual) and the source of the information (unless already known by the Individual);

- The purpose of Processing or collecting the Personal Information and the legal basis (or bases) for the Processing:
    - if the legal basis is legitimate interest, the notice must specify that interest;
    - if the legal basis is a legal obligation or contractual requirement, the notice must indicate if the Individual is obligated to provide the Personal Information and the possible consequences if the Individual chooses not to provide the data;
    - if the lawful basis is consent, the right to withdraw consent at any time without affecting the lawfulness of the Processing based on consent before its withdrawal, as well as information about the impact of the withdrawal;
- The recipients or categories of recipients with whom the Personal Information will be shared;
- Whether the Personal Information will be shared across borders and, if so, whether the Personal Information will be sent to countries that lack an adequacy decision, a reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- How long the data will be retained;
- Their rights to request access, rectification, erasure and restriction of Processing and the rights to object, data portability, and lodge a complaint with a Supervisory Authority (for Individuals and Personal Information subject to the GDPR); and
- The logic, possible consequence, and means to seek redress, if the Personal Information is subject to automated decision-making.

All Operating Businesses shall comply with the requirements of Articles 12 and 13 of the GDPR when providing notice to the extent that the GDPR applies.

Where Operating Businesses obtain Personal Information indirectly, they will inform Individuals (as described above) in accordance with Article 14(3) GDPR, unless the Individual has already been informed or another derogation of Article 14(5) GDPR would apply.

For ease of reference, Exhibit E of these BCRs provides the full text of Articles 13 and 14 GDPR.

d) *Respect the legitimate rights of Individuals to exercise their privacy rights over their Personal Information*

Otis shall allow Individuals to request access to and rectification of their Personal Information. The Corporate Office and/or the relevant Operating Business will comply with requests, provided such requests are not manifestly unfounded or excessive, without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Corporate Office and/or the relevant Operating Business will inform the Individual of any such extension within one month of receipt of the request, together with the reasons for the delay, as well as any refusal to comply with a request and the reason for the refusal. The Corporate Office and/or the relevant Operating Business shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. Individuals may be required to provide proof of their identity and may be subject to a servicing fee as permitted under the GDPR.

Individuals may object to the Processing of their Personal Information or request the restriction of Processing or erasure of their Personal Information. Otis will comply with such requests, unless Processing of Personal Information is required by regulatory or legal obligations, to defend the company against legal claims, or on compelling legitimate grounds that override the interests and rights of Individuals, such as corporate audits. Individuals will be informed of the consequences that may arise as a result of their choice to have Otis not Process their Personal Information, such as the inability of Otis to provide employment, a requested service or enter into a transaction. Individuals will also be informed about the outcome of their request and will be reminded of their right to submit a complaint in accordance with Section D.5(c) of these BCRs.

Individuals have the right to object at any time to Processing of Personal Information for marketing purposes. Individuals who do not wish to receive marketing communications from Otis will be offered easily accessible means to oppose further advertising, for example, in their account settings or by following the directions provided in an email or from a link in the communication. When in doubt about the application of anti-spam regulations, please contact **privacy@otis.com**.

Individuals have the right not to be subject to a decision based solely on automated Processing, including profiling. Where Otis makes automated decisions about Individuals on the basis of their Personal Information, it shall provide suitable measures to safeguard Individuals' legitimate interests, such as providing information about the logic behind the decision and an opportunity to have the decision reviewed by human intervention and permitting Individuals' to provide their point of view and to contest the decision.

e) *Implement appropriate technical and organizational security measures*

Otis shall implement appropriate security measures taking into account the sensitivity and risks of the Processing concerned, the nature of the Personal Information concerned and

applicable corporate policies. These security measures may include, as appropriate, pseudonymization and encryption, processes to ensure the confidentiality, integrity, availability and resilience of processing systems, sufficient back-ups to reasonably guarantee availability and access, and regular audit and testing of the security measures in place.

Operating Businesses shall implement a robust Data Breach Incident Response Plan or adhere to Otis's Data Breach Incident Response Plan, which shall address the appropriate response to and remediation of any actual Data Breaches.

The Data Breach Incident Response Plan shall, at a minimum, require the Operating Businesses to:

(1.) provide notice, without undue delay, to the Otis Lead Entity and any other relevant internal privacy function, and, in accordance with Articles 33 or 34 of the GDPR, to the Supervisory Authorities within 72 hours, and/or affected Individuals, without undue delay;

(2.) follow an appropriate investigatory process, including documenting the Incident, the investigation, and the remediation; and

(3.) make the documentation of the Incident available to a Supervisory Authority upon request. The Operating Businesses shall follow the Data Breach Incident Response Plan.

Otis will enter into a written agreement obligating any internal or external Service Providers to respect these BCRs or equivalent requirements and only to Process Personal Information in accordance with the instructions of Otis. The written agreement must use the standard terms and conditions provided by Otis or have any modifications approved by the designated Business Unit Privacy Professional or the Otis Privacy Lead. For those agreements covering services involving Personal Information subject to the GDPR, the agreement shall comply with the requirements of Article 28 GDPR, and the standard terms and conditions shall include a template that complies with the Article 28 requirements. For ease of reference, Exhibit E of these BCRs provides the full text of Article 28 GDPR.

f) *Not transfer Individuals' Personal Information to Third Parties or Service Providers outside the EEA without appropriate safeguards*

Otis shall only transfer Individuals' Personal Information to Third Parties or to Service Providers that are not bound Operating Businesses if such Third Parties or Service Providers are: (1) located in countries that provide adequate levels of protection (as defined by Article 45 GDPR); (2) have other arrangements that would satisfy EU adequacy requirements as set forth in Article 46 GDPR; or (3) fully comply with one of the derogations (exceptions) listed in Article 49 GDPR – all in accordance with Article 48 GDPR. For ease of reference, Exhibit E of these BCRs provides the full text of Articles

46, 48 and 49 of the GDPR. In all instances in which transfers are made to Service Providers, Otis shall ensure appropriate contract terms are in place as set forth above in Section D.1.e.

g) *Implement Appropriate Accountability Measures*

Every Operating Business acting as Controller shall be responsible for and able to demonstrate compliance with the BCRs. Operating Businesses shall comply with accountability requirements such as keeping a record of Processing operations, (which, for Personal Information originating directly or indirectly from the EEA shall have the various elements listed in Article 30 (1) GDPR), carrying out data protection impact assessments where this would be required under the GDPR, and implementing appropriate technical and organizational measures to meet the principles of privacy by design and privacy by default. Any Personal Information data inventories involving EEA Personal Information shall be made available to the competent Supervisory Authority upon request. For ease of reference, Exhibit E of these BCRs provides the full text of Article 30 GDPR. For any data protection impact assessment completed in accordance with Article 35 GDPR that indicates that the Processing would result in a high risk that cannot be properly mitigated, Otis shall ensure that the competent Supervisory Authority is consulted in accordance with Article 36 GDPR.

2. Governance: Otis commits to maintain a governance infrastructure capable of ensuring compliance with the BCRs. This infrastructure consists of:

a) *Ethics and Compliance Officers*: these Officers facilitate compliance with the BCRs and are the internal point of contact for internal comments and complaints relating to the BCRs. Otis will ensure that its Ethics and Compliance Officers are trained to receive and investigate privacy complaints, to assist with the resolution of privacy concerns, and to forward complaints to the appropriate resources, such as the appropriate Privacy Professional or the Privacy Office, for review and resolution where needed.

b) *Privacy Professionals*: each Business Unit will appoint at least one Privacy Professional to serve as a resource for the Ethics and Compliance Officers and others in the Business Unit with privacy-related issues. The Privacy Professionals assist their management in ensuring local compliance with these BCRs and in identifying and remediating shortcomings within the Business Unit. Otis will ensure that these Privacy Professionals have sufficient resources and independent authority to perform their role.

c) *Data Protection Officers ("DPOs")*: the role of the DPO is defined by applicable law. DPOs are appointed where required by applicable law. DPOs coordinate on a regular basis with the Otis Privacy Lead.

d) *Otis Privacy Council ("OPC")*: the OPC will be responsible for general oversight of Otis's privacy compliance program, including the implementation of the BCRs. The OPC will contain the Privacy Professionals, representing their respective Business Unit, as well as

representatives from Human Resources ("HR"), Information Technology ("IT"), International Trade Compliance ("ITC"), Environmental, Health & Safety ("EH&S"), Finance, Supply Management, and Otis Lead Entity. Other members may be added either temporarily or permanently, as needed. The OPC, in cooperation with the Otis Privacy Lead and the Privacy Office, develops and ensures global implementation of compliance plans to address the findings of the assurance and audit teams.

e) *Global Head of Data Privacy (Privacy Lead)*: the Privacy Lead, in cooperation with the Privacy Professionals, will deploy the BCRs and ensure that they are effectively and efficiently implemented. The Privacy Lead will also be responsible for training and awareness campaigns on data privacy and for supporting the Privacy Professionals and ensuring that they are trained, while promoting the existence and purpose of data privacy requirements in addition to basic requirements for the protection of proprietary information. The Privacy Lead will provide direction to and lead the Otis Privacy Council. The Privacy Lead will serve as the Privacy Professional for the Corporate Office and has access to and reports to the highest level of management (*i.e.*, the Board of Directors), and shall have support from the highest level of management.

f) *Privacy Office*: the Privacy Office consists of the Privacy Lead, the Privacy Professionals, and any appointed Data Protection Officers, as well as any additional personnel appointed by the Operating Businesses or the Corporate Office. The Privacy Office participates on the OPC, responds to and resolves any comments or complaints that come into the Privacy Office, and assists the Ethics and Compliance Officers in responding to and resolving any comments or complaints that are submitted to the Ethics and Compliance Officer team.

g) *Otis Lead Entity*: the Otis Lead Entity will participate on the OPC through its Privacy Professional or DPO. In case of evidence of violations of the BCRs, the OPC or the Privacy Lead will inform Otis Lead Entity and, in coordination with Otis Lead Entity, work with the Corporate Office and/or the relevant Operating Business and its Privacy Professional to implement appropriate remediation steps.

3. Training: Otis will ensure that the following categories of Personnel receive annual training on data privacy (including relevant aspects of these BCRs), security, and/or anti-spam regulations:

- Ethics and Compliance Officers;
- Privacy Professionals;
- Personnel who have permanent or regular access to Personal Information and handle Individuals' Personal Information as an integral part of their responsibilities; and
- Personnel involved in the development of tools used to Process Personal Information.

4. Monitor and Audit: The Otis Vice President, Internal Audit, supervising the internal audit program, will administer assurance and audit programs on at least a quarterly basis to evaluate

compliance with all aspects of these BCRs, and will follow up with the Operating Businesses to ensure that corrective measures are taken. The Otis Vice President, Internal Audit, with the assistance of the internal audit staff, the Privacy Lead, and the Operating Businesses, will determine the appropriate scope and regularity of the audit program for BCRs (including ad-hoc audits, as necessary) to address systems and processes that must adhere to these BCRs.

Results of the BCRs compliance audits will be communicated to the Privacy Lead, who, in turn, will inform the Otis Vice President, General Counsel, Otis Lead Entity, and the Otis Privacy Council. The Otis Vice President, General Counsel, together with the Otis Vice President, Internal Audit, will communicate material audit findings related to the BCRs to the Board of Directors or a committee of the Board, such as the Audit Committee. Competent Supervisory Authorities in the EEA, upon request, may receive access to the audit results related to the BCRs.

5. **Handling Requests for Rights and Complaints:** Requests from Individuals regarding the Processing of their Personal Information will be addressed as set out below. These contact methods may be supplemented where required by local law. Irrespective of the procedures described below, Individuals whose Personal Information originates directly or indirectly from the EEA maintain the right to submit a complaint directly to a Supervisory Authority and/or a competent court.

a) Internal - From Personnel with access to Otis's Intranet

Personnel who are direct Otis employees can address their requests and complaints to their local Human Resources representative. All Personnel, including employees, may contact their Ethics and Compliance Officer, Complaint Reporting, or the Privacy Office. These resources can be contacted as follows:

Local HR	Contact using your regular internal channels
Ethics and Compliance Officers	Contact using your regular internal channels: https://connect.otis.com/business_practices/Pages/default.aspx
Complaint Reporting	Contact using your regular internal channels or report to: **www.otis.com/reportingchannel**
Privacy Office	**privacy@otis.com**

Complaints submitted to local HR, Ethics and Compliance Officers, or the Privacy Office: these complaints will be addressed by the group (HR, Ethics and Compliance Officers, or Privacy Office) that has received them, with assistance from the appropriate Privacy Professional or the Privacy Lead (or designee) where needed.

Privacy complaints submitted to Complaint Reporting: so long as the complainant seeks a further response and agrees, those complaints will be forwarded to the Privacy Office for response and resolution.

b) External - From all other Individuals

Requests and complaints from all other Individuals can be addressed to Complaint Reporting or the Privacy Office, which can be reached as follows:

Complaint Reporting	Diane Andrews, Global Privacy Counsel
Privacy Office	**privacy@otis.com**

So long as the complainant seeks a further response and agrees, privacy complaints submitted to Complaint Reporting will be forwarded to the Privacy Office for response and resolution.

c) Complaint Response

The group that has received the complaint (hereinafter the "respondent") is responsible for providing a written response (email is acceptable, unless otherwise requested by the Individual). In instances where more information is required, either to authenticate the identity of the complainant or to understand the nature of the complaint, the respondent will contact the complainant to seek additional information as appropriate. Where the complainant does not respond or is unable to establish reasonable verification of identity, the respondent may communicate to the complainant within 1 month that Otis deems the complaint to be closed.

If the complaint is deemed to be justified, Otis will work to remedy the issue and communicate the solution to the complainant. If the complainant is not satisfied with the solution, Otis will remind the complainant of the right to submit a complaint with the Supervisory Authority and/or a competent court.

Where the complaint is deemed unjustified, the respondent must provide the complainant with a written explanation and notification that the complainant is able to submit a complaint with the Supervisory Authority and/or a competent court.

If the respondent is unable to reach a solution (for a justified complaint) or provide an explanation (for an unjustified complaint) that satisfies the complainant, the respondent must report the issue to the Privacy Lead. The Privacy Lead will review the complaint and response to determine if further action is appropriate.

Complaints and audit results revealing structural shortcomings globally will be addressed by Privacy Lead through the OPC in order to ensure a global resolution in cooperation with Otis Lead Entity and the local Privacy Professionals.

The period for providing a response should not exceed one month, unless the complexity and scope of the request/complaint are such that more time is needed, in which case the response may be postponed by another two months, after having informed the Individual of the reason of the delay.

No provision of the BCRs shall affect the rights of Individuals under applicable local law to submit a complaint to a competent Supervisory Authority or court in relation to a breach of applicable law by an Operating Business that is located in the EEA.

For alleged breaches of these BCRs, Individuals may:

- file a complaint with a competent Supervisory Authority, in particular, in the country of the Individual's habitual residence, place of work or place of the alleged infringement; or
- bring an action before a competent EEA court, either the court where the Controller or processor has an establishment or where the Individual has his or her habitual residence, at the Individual's choice.

6. Enforcement Rights of Individuals and Guarantees: Subject to the limitations described in the section Scope (Section C), Individuals shall have the benefit of the rights (third party beneficiary rights) expressly granted to them pursuant to this Section, Sections B, C, D.1, D.5, D.7, D.8 and D.9, and the benefit of the guarantee given by the Otis Lead Entity (Otis Elevator Worldwide BVBA[2]) in this Section.

All Individuals who otherwise have rights under these BCRs have recourse to the statutory redress procedures provided under their applicable national law. Operating Businesses located outside the EEA and that violate these BCRs agree that the courts or other competent authorities in the EEA have jurisdiction over alleged BCRs violations, and the Individual will have the rights and remedies against the Otis Lead Entity as if the violation had been caused in the Member State where the Otis Lead Entity is established.

With assistance from the Otis Corporate Office, the Otis Lead Entity shall be responsible for ensuring that actions are taken (1) to remedy a breach committed by the Otis Corporate Office or the Operating Businesses outside of the EEA; and (2) to pay the compensation to Individuals awarded by courts referred to in this section for any material or non-material damages or fines resulting from the breach of the BCRs by the Corporate Office and/or an Operating Business outside the EEA, unless the relevant Operating Business has already remedied the breach or paid the compensation.

Where Individuals can demonstrate that they have suffered damage, then it shall be for Otis Lead Entity, in cooperation with the Otis Corporate Office, to prove that the Corporate Office

[2] With registered address at 58, Avenue des Arts, 1000 Brussels, Belgium, and [registration number –0652.780.207.

and the Operating Business concerned was not in breach of its obligations under these BCRs. Where such proof can be provided, Otis Lead Entity may discharge itself of any responsibility under the BCRs.

For countries other than the EEA Member States, which recognize these BCRs as a lawful instrument to transfer Personal Information, Individuals in those countries shall have the benefit of the rights expressly granted to them pursuant to Sections D.1, D.5, D.7 and D.9. Accordingly, affected Individuals in these countries may take any action in their country to enforce these provisions against the Operating Business in breach of the BCRs.

7. **Cooperation with Supervisory Authorities:** Operating Businesses shall provide any assistance required by competent Supervisory Authorities in connection with their enquiries and verifications in relation to the BCRs, including providing the results of audits upon request.

Otis shall abide by the decisions of competent EEA Supervisory Authorities and advice it receives from Supervisory Authorities related to the BCRs. Otis accepts that its compliance with the BCRs may be audited by competent Supervisory Authorities in compliance with EEA applicable laws.

8. **Modification to these BCRs:** Otis Lead Entity shall promptly notify the Belgian Supervisory Authority in the event that any amendment or variation is made to these BCRs that materially alters the level of protection as set out therein; once a year, Otis Lead Entity shall notify the Belgian Supervisory Authority of all changes that occurred in the previous year with a brief explanation justifying the changes. Otis shall also undertake to inform without undue delay all bound Operating Businesses of any changes by notifying the OPC, including all Privacy professionals and DPOs, who shall in turn notify the bound Operating Businesses.

Otis Privacy Lead shall maintain an up-to-date list of all Operating Businesses that have executed the Intra-Group Agreement and of all updates of the BCRs. Such list shall be made available to bound Operating Businesses, Individuals, and EEA Supervisory Authorities, upon request. In any event, the Otis Privacy Lead or Otis Lead Entity shall provide the Belgian Supervisory Authority with a copy of an up-to-date list of all Operating Businesses that have executed the Intra-Group Agreement not less than once per year.

Otis agrees that it shall not rely upon these BCRs to transfer Individuals' Personal Information to other members of the Otis group until such time as the relevant group members have executed the Intra-Group Agreement and can comply with it. Otis shall make no transfer to a new BCRs member until the new BCRs member is effectively bound by the BCRs and can deliver compliance. Where a non-EEA BCRs member ceases to be part of the group or to be bound by the BCRs, its obligations arising under the BCRs with respect to any Personal Information originating directly or indirectly from the EEA received while bound by the BCRs shall persist until such time as the relevant Personal Information is either returned, deleted, expunged or anonymized.

9. **Communication of these BCRs:** With the intention of ensuring that Individuals are made aware of their rights under these BCRs, the Operating Businesses shall post or maintain a link to these BCRs on their external-facing websites. Otis shall post or maintain a link to these BCRs on **www.otis.com** or any superseding website.

EXHIBIT A - DEFINITIONS

"Business Unit" means Otis' major segments, which may change from time to time, and currently consistent of North America, Latin America, EMEA, Asia Pacific, China, and the Otis Corporate Office.

"Consent" means any freely given, specific, informed and unambiguous indication of an Individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Information relating to him or her.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.

"Corporate Office" refers to the company's corporate headquarters in the U.S. at One Carrier Place, Farmington, CT 06032 USA.

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed.

"EMEA" means Europe, Middle East, and Africa.

"GDPR" means the General Data Protection Regulation.

"Individual" means a natural person whose Personal Information is Processed by Otis.

"Operating Businesses" means Otis' business segments, units and divisions, and all other operating entities wherever located (including controlled joint ventures, partnerships and other business arrangements where Otis has either a controlling interest or effective management control), other than the Corporate Office.

"Personal Information" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Personnel" means Otis employees, including Otis directors and officers, and temporary employees, contractors, leased labor and contract laborers retained by Otis.

"Processing" (including its cognate forms) means any operation or set of operations which is performed on Personal Information, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, transfer, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Sensitive Personal Information" is a subset of Personal Information revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; as well as the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sexual orientation or sex life; or the commission or alleged commission of any crime and possible penalties.

"Service Provider" or **"Processor"** means any entity or person who/that on behalf of Otis Processes, or otherwise is permitted access to Personal Information Processed by Otis through its provision of services directly to Otis.

"Supervisory Authority" shall have the same meaning as set forth in the GDPR.

"Otis" means Otis's Corporate Office and its Operating Businesses.

EXHIBIT B - INTERNAL PROCESSING CLAUSES

These clauses apply when an Operating Business that is bound by the BCRs (hereafter: the "Otis Principal") entrusts a project to another bound Operating Business (hereafter: the "Otis Processor") that involves the processing of covered Personal Information. To the extent that the project involves a written document ("Work Order") between Otis Principal and Otis Processor, the Work Order shall reference the Internal Processing Clauses in the following terms: "The Services set out in this Work Order are governed by the Internal Processing Clauses set out in the Otis BCRs for the protection of personal information."

Defined terms in these clauses refer to the defined terms in the Otis BCRs.

1. Otis Principal and Otis Processor agree to remain bound by the Otis BCRs for the entire duration of the Work Order. These clauses apply for the duration of the Work Order. The provisions of Section 4.2, 4.4, 4.5., 4.8., 4.10 and 4.11 of these clauses shall survive termination of the Work Order.

2. In the performance of its services, Otis Processor will process Personal Information on behalf of Otis Principal.

3. Obligations of Otis Principal:

   3.1. Otis Principal shall provide Otis Processor with clear instructions relating to the nature, purpose and duration of the processing of relevant Personal Information. These instructions shall be sufficiently clear to allow Otis Processor to meet its obligations under these clauses and the Otis BCRs. In particular, Otis Principal's instructions may govern the use of sub-contractors, the disclosure of Personal Information and other obligations of Otis Processor.

   3.2. Otis Principal shall inform Otis Processor about all amendments to its national data protection law and related statutory instruments, regulations, orders, and similar instruments that are of relevance to the Processing performed by Otis Processor under these clauses, and provide instructions on how Otis Processor should comply with such amendments.

4. Obligations of the Otis Processor

   4.1. Otis Processor shall Process Personal Information in accordance with the instructions of Otis Principal as set forth in the Work Order and as communicated in writing. Otis Processor shall not carry out Processing of relevant Personal Information for any other purpose or in any other manner.

   4.2. Otis Processor shall comply with all provisions of the Otis BCRs and in particular with Section D.1.e.

4.3. Otis Processor shall not disclose or transfer relevant Personal Information to any third party, other than a sub-processor pursuant to Section 4.6 of these clauses, without the prior authorization, in writing, of Otis Principal.

4.4. Where, in accordance with the Otis BCRs (Section D.1.f.), Otis Processor is required to carry out Processing as a result of a valid legal obligation, it shall do so notwithstanding the requirements of this Section 4. In such cases, Otis Processor shall notify Otis Principal in writing prior to complying with any such requirement, unless the applicable law, regulation, or governmental authority prohibits the providing of such notice, and shall comply with all reasonable directions of Otis Principal with respect to such disclosures.

4.5. Otis Processor shall notify Otis Principal within three (3) business days of any communication received from any individual whereby that individual exercises his or her rights relating to Personal Information of him or her and shall comply with all instructions of Otis Principal in responding to such communications. In addition, Otis Processor shall provide any and all assistance required by Otis Principal to respond to any communication from any individual relating to that individual's rights on Personal Information relating to him or her.

4.6. Otis Processor may engage a sub-processor to assist it in fulfilling its obligations under the Work Order provided it has obtained the prior written approval of Otis Principal. Otis Processor will enter into a written agreement with any sub-processor, which imposes obligations on the sub-processor that are no less onerous than and comparable in all material respects with the obligations imposed upon Otis Processor under these clauses. Otis Processor must comply with Otis BCRs Section D.1.f.

4.7. Otis Processor represents and warrants that nothing in any data protection legislation (or any other laws or regulations) to which it is subject, prevents it from fulfilling its obligations under these clauses. In the event of a change in any such laws that is likely to have a substantial adverse effect on Otis Processor's compliance with these clauses or in the event Otis Processor otherwise cannot comply with these clauses, Otis Processor shall notify Otis Principal within fifteen (15) business days and Otis Principal shall be entitled to terminate the Work Order with immediate effect.

4.8. Otis Processor agrees that Otis Principal may request that Otis Processor's compliance with these clauses is audited in accordance with Otis BCRs Section D.4. In particular, Otis Processor shall make available to Otis Principal all information necessary to demonstrate its compliance with these obligations and submit to audits, including inspections, conducted by Otis principal or an auditor mandated by Otis Principal.

4.9. Otis Processor shall ensure that any person Processing Personal Information under the authority of Otis Processor is subject to suitable duties of confidentiality.

4.10. Otis Processor shall assist Otis Principal in complying with its obligations under applicable data protection laws, including in completing data protection impact assessments and consulting with Supervisory Authorities, where applicable.

4.11. Otis Processor shall notify Otis without undue delay of the occurrence of a data breach and shall promptly take steps to rectify and prevent recurrence of the data breach, and assist Otis in doing the same where required. Otis or the appropriate Operating Business will coordinate with Otis Principal and Otis Processor regarding the appropriate investigation and remediation. Otis Processor shall also assist Otis Principal as may be necessary to fulfil Otis Principal's obligation to notify a government authority or affected individuals about the data breach.

4.12. Otis Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk to Personal Information that it Processes on behalf of Otis Principal, in accordance with Section D.1.e of the Otis BCRs.

5. In the event of the termination of the Work Order, Otis Processor shall send to Otis Principal all relevant Personal Information held by Otis Processor, together with all copies in any media of such data or destroy the same, unless Otis Processor is required, by any applicable law, regulation or governmental authority, to retain such Personal Information or a part thereof, in which case it shall promptly notify Otis principal of any such obligation.

6. These clauses shall be governed by and construed in accordance with the laws of the country in which Otis Principal is established. Without prejudice to Otis BCRs Section D.6, each party to these clauses irrevocably submits to the exclusive jurisdiction of the country of Otis Principal's courts over any claim or matter arising under or in connection with these clauses.

7. Miscellaneous

7.1. The provisions of these clauses are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of these clauses shall remain in full force and effect.

7.2. The provisions of these clauses shall inure to the benefit of and shall be binding upon Otis Principal and Otis Processor and their respective successors and assigns.

EXHIBIT C – LIST OF BOUND ENTITIES

List of bound entities available upon request – for requests or inquiries please email **privacy@otis.com**.

EXHIBIT D

Description of Types Personal Information Processed by Otis

This table summarizes the main types of Personal Information that Otis may Process across its business lines. The types of Personal Information listed below will be collected depending on the scenario, and will always be done in accordance with the law and local legal requirements, including with regard to Sensitive Personal Information as stated elsewhere in these BCRs.

Types of Personal Information
Name(s): Name, including given, family, middle, any suffix (such as Junior or Senior), and salutation (such as Mr. or Ms.)
Identification details: Date of birth, gender, and government-issued identification (including passports and visas); country of birth, citizenship and residency status, all in accordance with applicable law.
Work contact and employer details: Information including work telephone numbers, fax number, work email address, mailing address, and work location; information about employer, including company name(s), company location(s), company address(es), and country of incorporation.
Personal contact details: Home address, personal email address and home telephone number, including personal mobile phone.
Emergency contact details: Information such as the name and contact details of the individual's spouse or close family member.
Background and career data: Work experience, education and job history, skill categories including language skills, licenses, certifications, authorization to perform a certain job, or memberships to and participation in trade associations or professional organizations; military service information as required by applicable requirements and law; information about work preferences, such as travel and location preferences.
HR and work-related data: Information such as an employee or contractor's: job title, department, job function, and cost center (as applicable); name of supervisor and/or assistant; work assignments and work product that may include a connection to an individual; work agreements, programs, and activities in which an individual participates; other data required to support human resources applications, including payroll, travel and expense administration; training, development, and/or performance review information; time collection and allocation information; information collected as part of an assignment, such as time and attendance, identification information, or geolocation data used for a particular role or assignment, and/or security clearance data (all in accordance with applicable law); succession planning information; tax-related information, such as marital status,

Types of Personal Information
relationship to policy holder, and/or dependents; information about health and injuries, such as disability, sickness leave, maternity leave, and other information that may be required to administer human resources and provide related benefits/services.
System access and IT security data: Otis computer, network, and communications information and logs covering the use of company phones, computers, electronic communications (such as email and electronic calendars), and other information and communication technology, including but not limited to username/login identification, passwords, answers to security questions, and other information required to access Otis applications, networks, systems, and services as well as information that an individual stores, sends, submits, or receives through Otis' networks and systems.
Physical security data: Information in relation to access to Otis' premises and to ensure physical safety and prevent unauthorized access, including access controls, disaster preparedness measures, and other necessary information.
EHS data: Information needed to ensure safety of Otis premises and comply with environment, health and safety laws, including record of incidents occurring on Otis premises or during work.
Product/service-related data: Information provided to facilitate a service or request assistance, such as product use or problem information, including location information for certain sites that provide location-based services; telematics data with respect to certain products; payment, invoice and financial data for the provision of a product or service; warranty-related information.
Website and app data: Information collected through use of Otis websites or apps, such as device identifiers, IP address, log files, and location data, all in accordance with applicable law.
Other data (as applicable): Language and communication preference(s); information that an individual volunteers to include in a profile in electronic systems; event registration information; visitor data, including time, date and location of a visit and approved or denied screening result (where applicable); listing of gifts that may have been provided or received to comply with applicable laws; information collected through a voluntary survey or promotion or through use of a product; other information that may be required for international trade compliance.

Description of Purposes for which Personal Information is Processed by Otis

This table summarizes the main purposes for which Otis may Process of Personal Information across its business lines.

Purpose	Individuals Whose Information is Processed					
	Employees and Outsourced Labor (as applicable)	**Job Applicants**	**Personnel of suppliers, vendors, and business customers**	**Visitors of Otis systems and facilities**	**Persons authorized to use Otis systems**	**Consumers and end users of certain Otis products**
Managing employment, including: compensation and benefits, including establishment and administration of benefit plans; payroll administration, such as for deductions and contributions; career development, performance feedback and progression; rewards and recognition; time collection and allocation; travel and expense reimbursement, including travel and/or credit card administration; training; relocations, letters of assignment, support for expatriate employees, visas, licenses and other right-to-work authorizations; tax reporting and withholdings; maintenance of employee and officer biographies and CVs; business planning; email systems and organizational charts; health and safety programs and health screenings; audits and compliance reviews; managing internal investigations.	Name(s); identification details; work contact and employer details; personal contact details; emergency contact details; background and career data; HR and work-related data; system access and IT security data; physical security data;					

Purpose	Individuals Whose Information is Processed					
	Employees and Outsourced Labor (as applicable)	Job Applicants	Personnel of suppliers, vendors, and business customers	Visitors of Otis systems and facilities	Persons authorized to use Otis systems	Consumers and end users of certain Otis products
	EHS data; physical security data; website and app data; other data					
Managing labor and employee relations, including grievance proceedings	Name(s); identification details; work contact and employer details; HR and work-related data; system access and IT security data; EHS data; physical security data; website and app data; other data					

Purpose	Individuals Whose Information is Processed					
	Employees and Outsourced Labor (as applicable)	**Job Applicants**	**Personnel of suppliers, vendors, and business customers**	**Visitors of Otis systems and facilities**	**Persons authorized to use Otis systems**	**Consumers and end users of certain Otis products**
Facilitating investor management activities	Work contact and employer details; HR and work-related data					
Staffing and staff succession planning, including as that may impact budget and financial planning and reporting	Work contact and employer details; HR and work-related data					
Protecting intellectual property rights, including but not limited to patent filings	Work contact and employer details; system access and IT security data		Work contact and employer details; system access and IT security data			
Conducting regular business operations, including designing and developing products, managing an Enterprise Resource Planning (ERP) system, sending invoices and collecting payment, providing payment, and providing goods and services to customers, which may include sharing	Name(s); work contact and employer details; HR and work-related data; product/ service		Name(s); work contact and employer details; product/ service related data; website and	Name(s); work contact and employer details; product/ service related data; website and	Name(s); work contact and employer details; product/ service related data; website and	Name(s); work contact and employer details; product/ service related data; website and

Purpose	Individuals Whose Information is Processed					
	Employees and Outsourced Labor (as applicable)	Job Applicants	Personnel of suppliers, vendors, and business customers	Visitors of Otis systems and facilities	Persons authorized to use Otis systems	Consumers and end users of certain Otis products
limited personal information with customers or other business partners	related data; website and app data; other data		app data; other data	app data; other data	app data; other data	app data; other data
Providing requested information, products and services, which may include use of geolocation for certain applications in a known and transparent manner	Product/ service related data;		Product/ service related data;			Product/ service related data;
Conducting and managing engagement surveys and charity campaigns	Other data					Other data
Reporting and statistical analyses, including global enterprise headcount, demographics, and reporting required by applicable law	Work and employer details; work-related data					Work and employer details
Responding to situations involving a risk of health or safety, including an emergency	EHS data; physical security data		EHS data; physical security data	EHS data; physical security data	EHS data; physical security data	EHS data; physical security data
Managing communications and notices	Name(s); work contact and employer details;		Name(s); work contact and employer details;	Name(s); work contact and employer details;	Name(s); work contact and employer details;	Name(s); work contact and employer details;

Purpose	Individuals Whose Information is Processed					
	Employees and Outsourced Labor (as applicable)	**Job Applicants**	**Personnel of suppliers, vendors, and business customers**	**Visitors of Otis systems and facilities**	**Persons authorized to use Otis systems**	**Consumers and end users of certain Otis products**
Managing physical security, including access controls and security, facility access and safety, and disaster preparedness	Name(s); work contact and employer details; system access and IT security data; EHS data; physical security data; other data		Name(s); work contact and employer details; EHS data; physical security data; other data	Name(s); work contact and employer details; EHS data; physical security data; other data	Name(s); work contact and employer details; EHS data; physical security data; other data	Name(s); work contact and employer details; EHS data; physical security data; other data
Managing, maintaining, and securing information technology ("IT") systems	Name(s); work contact and employer details; system access and IT security data		Name(s); work contact and employer details; system access and IT security data	Name(s); work contact and employer details; system access and IT security data	Name(s); work contact and employer details; system access and IT security data	Name(s); work contact and employer details; system access and IT security data
Ensuring compliance with import, export, and other international trade controls, including managing registrations and authorizations, determining access to controlled technologies and/or commodities,	Name(s); identification details; work contact and employer details		Name(s); identification details; work contact and employer details	Name(s); identification details; work contact and employer details	Name(s); identification details; work contact and employer details	Name(s); identification details; work contact and employer details

Purpose	Individuals Whose Information is Processed					
	Employees and Outsourced Labor (as applicable)	**Job Applicants**	**Personnel of suppliers, vendors, and business customers**	**Visitors of Otis systems and facilities**	**Persons authorized to use Otis systems**	**Consumers and end users of certain Otis products**
and screening for sanctioned or restricted countries or parties						
Prosecuting and defending claims and responding to law enforcement requests (where so required and only in accordance with applicable law)	Any categories required by law or needed for this purpose	Any categories required by law or need for this purpose	Any categories required by law or needed for this purpose	Any categories required by law or needed for this purpose	Any categories required by law or needed for this purpose	Any categories required by law or needed for this purpose
Providing customer service and support, Training and certification of customer, supplier, and vendor personnel, and conducting due diligence and risk assessments			Name(s); work contact and employer details; other data	Name(s); work contact and employer details; other data	Name(s); work contact and employer details; other data	Name(s); work contact and employer details; other data
Purposes related to the use of Otis' websites and apps, including responding to requests or further processing forms submitted; advertise products, services, promotions and events related to Otis; improving our products, services, websites and apps; protecting against fraud or investigate suspected or actual illegal activity; developing new offerings, improve the quality of our products, improve and personalize user experience.	Name(s); work contact and employer details; website and app data	Name(s); work contact and employer details; website and app data	Name(s); work contact and employer details; website and app data	Name(s); work contact and employer details; website and app data	Name(s); work contact and employer details; website and app data	Name(s); work contact and employer details; website and app data

Purpose	Individuals Whose Information is Processed					
	Employees and Outsourced Labor (as applicable)	**Job Applicants**	**Personnel of suppliers, vendors, and business customers**	**Visitors of Otis systems and facilities**	**Persons authorized to use Otis systems**	**Consumers and end users of certain Otis products**
Job application purposes, including: receiving applications for employment; evaluating applications; arranging for and conducting phone screenings interviews, and other applicable assessments; contacting an applicant with about an application or other opportunity; communicating changes; validating reference checks, conduct background checks (as appropriate in accordance with applicable law); screening; facilitating hiring; complying with legal and regulatory requirements; ; verifying identity to ensure security; providing feedback opportunities; and conducting analysis on applicant trends to understand and improve Otis' recruitment practices.		Name(s); identification details; work contact and employer details; personal contact details; background and career data; website and app data				