

Binding Corporate Rules

- A. INTRODUCTION
- B. APPLICABILITY
- C. SCOPE
- D. POLICY
- E. REFERENCES
- F. REVIEW

Issued: May 15, 2017
Last reviewed: December 3, 2018
Last Revised: December 3, 2018

A. INTRODUCTION

UTC 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.

UTC has adopted Binding Corporate Rules (“BCRs”) for the Personal Information that it Processes about Individuals. UTC Fire & Security EMEA BVBA (“UTC F&S”)¹ is the Lead Affiliate and, in coordination with the UTC 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.

UTC 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 UTC 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 and CCS products and services by users of those products and services. Personal Information is transferred within UTC 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 UTC Corporate Office, located in the U.S.

B. APPLICABILITY

1. These BCRs are mandatory for UTC’s Corporate Office and the Operating Businesses that have executed the Intra-Group Agreement. These entities shall ensure that their Personnel comply with these BCRs when Processing an Individual’s Personal Information. UTC will establish clear and consistent controls across the enterprise to ensure compliance with the BCRs.
2. At a minimum, UTC 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 UTC 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 UTC’s Corporate Office or one or more Operating Businesses from fulfilling their obligations under the BCRs and has a substantial effect on the guarantees provided therein, the entity concerned shall promptly notify the UTC Associate General Counsel, Data Privacy and Security (“AGC DPS”), except where providing such information is prohibited by a law enforcement authority or law. The UTC AGC DPS, in cooperation with the Privacy Advisory Committee and the entity and Business Units

¹ UTC Fire & Security EMEA BVBA, De Kleetlaan 3, 1831 Diegem, Belgium.

concerned, shall determine the appropriate course of action and, in case of doubt, consult with the competent data protection authority.

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 UTC entities. 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 Corporate Policy Manual Section 24, these BCRs prevail for Personal Information originating directly or indirectly from the European Economic Area or Switzerland.

C. SCOPE

These BCRs govern the Processing by UTC of Personal Information of Individuals wherever located, except that (i) the requirement to obtain explicit consent for Sensitive Personal Information, (ii) the provisions contained in Section D.6, paragraphs 1 through 6 regarding the enforcement rights of individuals and guarantees, (iii) Section B.4 relating to discrepancies between the BCRs and Corporate Manual Section 24, (iv) the requirements of D.1(d); and (v) the part of Section D.1(f) relating to sharing of data with law enforcement and regulatory authorities, shall only apply to Personal Information originating directly or indirectly from the European Economic Area, the United Kingdom or Switzerland.

D. POLICY

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

a) *Process Personal Information fairly and lawfully*

Individuals' Personal Information shall be Processed for identified purposes (1) on the basis of consent; (2) when required or permitted by law in the country of origin, or (3) for a legitimate purpose, such as human resources management, business interactions with customer and supplier, and 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 the Individual or the establishment, exercise, or defense of a legal claim by the Corporate Office or an Operating Business.

Individuals' Personal Information shall not be Processed for any incompatible purposes unless allowed under one of the conditions set out in the immediately preceding paragraph, for example, by obtaining a new consent.

b) *Only Process Personal Information that is relevant*

UTC shall make efforts to ensure that the Processing of Individuals' Personal Information is adequate, relevant and not excessive in relation to the purpose or purposes for which the information is Processed. In addition, UTC 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 by applicable law, regulation, court proceedings, administrative proceedings, arbitration proceedings, or audit requirements. UTC will make efforts to ensure that the Individuals' Personal Information in its possession 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 Personal Information that is to be collected; the identity and contact details of the UTC entity or entities responsible for the collected Personal Information; the contact details of the data protection officer, where applicable; the purpose(s) for which that Personal Information is to be collected; the legal basis for processing and the legitimate interest pursued by the controller, where applicable; the categories of recipients with whom UTC will share the information; the choices and rights provided to Individuals, including the right to withdraw consent or oppose the use of certain data and the right to file a complaint with the competent supervisory authority, where applicable; the consequences of exercising those choices; how to contact UTC with questions or complaints about privacy matters; the retention period of the collected data , where applicable; information on automated decision making, if any, where applicable, , the fact that UTC may share some of the collected data with recipients located outside of the EU and how UTC intends to protect the data, where applicable. In exceptional cases, where providing this notice presents a disproportionate burden (where the Personal Information was not obtained from the Individuals themselves), UTC may, after careful consideration, decide not to provide notice to Individuals or to postpone providing notice.

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

UTC 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 in a reasonable period of time, provided such requests are not manifestly unfounded or excessive. 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 by applicable law.

Individuals may object to the Processing of their Personal Information or request the blocking or erasure of their Personal Information. UTC will comply with such requests, unless retention of Personal Information is required by contractual obligations, audit requirements, regulatory or legal obligations, or to defend the company against legal claims. Individuals will be informed of the consequences that may arise as a result of their choice to have UTC not Process their Personal Information, such as the inability of UTC to provide employment, a requested service or enter into a transaction. Individuals will also be informed about the outcome of their request.

With the exception of those Individuals who have elected not to receive certain communications and in accordance with applicable law, UTC may Process Individuals' Personal Information to target communications to Individuals based on their interests. Individuals who do not wish to receive marketing communications from UTC 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.compliance@utc.com.

Where UTC 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 and permitting Individuals' to provide their point of view.

e) *Implement appropriate technical and organizational security measures*

In order to prevent unauthorized or unlawful Processing of Personal Information and to prevent accidental alteration, unauthorized disclosure or access, loss or destruction of, or damage to Personal Information, UTC 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. Operating Businesses shall implement a robust Data Breach Incident Response Plan or adhere to UTC's Data Breach Incident Response Plan, which shall address the appropriate response to and remediation of any actual Data Breaches.

UTC will enter into a written agreement obligating any Service Providers to respect these BCRs or equivalent requirements and only to process Personal Information in accordance with the instructions of UTC. The written agreement must use the standard terms and conditions provided by UTC or have any modifications approved by the designated Business Unit Privacy Professional or the UTC AGC DPS.

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

Where UTC transfers Individuals' Personal Information to Third Parties or to Service Providers that are not part of UTC and that are (1) located in countries that do not provide adequate levels of protection (within the meaning of the Directive 95/46/EC), (2) not covered by approved binding corporate rules, or (3) do not have other arrangements that would satisfy EU adequacy requirements, the Corporate Office and/or the relevant Operating Business shall ensure in relation to:

- Third Parties, that they shall implement appropriate contractual controls, such as model contractual clauses, providing levels of protection commensurate with these BCRs or, alternatively, ensure that the transfer (1) takes place with the unambiguous consent of the Individuals, (2) is necessary to conclude or perform a contract concluded with the Individuals, (3) is necessary or legally required on important public interest grounds², (4) is necessary to protect the vital interests of the Individuals; or (5) is necessary for the establishment, exercise or defense of legal claims.
- Processors, that they shall implement contractual controls, such as model contractual clauses, providing levels of protection commensurate with these BCRs.

g) *Implement Appropriate Accountability Measures*

Operating Businesses acting as data controllers or processors for Personal Information subject to the EU General Data Protection Regulation and the United Kingdom shall comply with accountability requirements such as keeping a personal information data inventory that shall record processing operations, carrying out data protection impact assessments and implementing the principles of privacy by design and privacy by default, where required by the General Data Protection Regulation. Any personal information data inventories involving EU Personal Information shall be made available to the competent supervisory authority upon request, as required by the General Data Protection Regulation.

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

- a) *Ethics and Compliance Officers (“ECO”)*: these Officers facilitate compliance with the BCRs and are the internal point of contact for internal comments and complaints relating to the BCRs. UTC 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

² In accordance with applicable law, Operating Businesses may share Personal Information with law enforcement and regulatory authorities when necessary in a democratic society to safeguard national and public security, defense, the prevention, investigation, detection and prosecution of criminal offenses and to comply with sanctions as laid down in international and/or national instruments.

appropriate Privacy Professional or the Privacy Office, for review and resolution where needed.

- b) *Ombudsman Program*: the individuals comprising the Ombudsman Program will maintain a mechanism to receive both internal and external comments and complaints relating to the BCRs. UTC's Ombudsman Program provides a safe and confidential channel for Individuals, Service Providers and Third Parties to seek guidance, ask questions, make comments and report suspected misconduct. The Ombudsman Program forwards complaints to the appropriate resources, such as the appropriate Privacy Professional or the Privacy Office, for review and resolution where needed, provided the complainant agrees.
- c) *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. UTC will ensure that these Privacy Professionals have sufficient resources and independent authority to perform their role.
- d) *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 UTC AGC DPS.
- e) *Privacy Advisory Committee ("PAC")*: the PAC will be responsible for general oversight of UTC's privacy compliance program, including the implementation of the BCRs. The PAC 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 UTC F&S. Other members may be added either temporarily or permanently, as needed. The PAC, in cooperation with the UTC AGC DPS and the Privacy Office, develops and ensures global implementation of compliance plans to address the findings of the assurance and audit teams.
- f) *UTC Associate General Counsel, Data Privacy and Security (AGC DPS)*: the AGC DPS, in cooperation with the Privacy Professionals, will deploy the BCRs and ensure that they are effectively and efficiently implemented. The AGC DPS 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 AGC DPS will provide direction to and lead the Privacy Advisory Committee. The AGC DPS will serve as the Privacy Professional for the Corporate Office.

- g) *Privacy Office*: the Privacy Office consists of the AGC DPS, 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 PAC, responds to and resolves any comments or complaints that come into the Privacy Office or the Ombudsman staff, and assists the ECOs in responding to and resolving any comments or complaints that are submitted to the ECO team.
- h) *UTC F&S*: UTC F&S will participate on the PAC through its Privacy Professional or DPO. In case of evidence of violations of the BCRs, the PAC or the AGC DPS will inform UTC F&S and, in coordination with UTC F&S, work with the Corporate Office and/or the relevant Operating Business and its Privacy Professional to implement appropriate remediation steps.
- 3. Training:** UTC will ensure that the following categories of Personnel, receive annual training on data privacy, security, and/or anti-spam regulations:
- Ethics and Compliance Officers;
 - Privacy Professionals;
 - Personnel handling 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 UTC Vice President, Internal Audit, supervising the Internal Audit Department, will administer regular assurance and audit programs to evaluate compliance with these BCRs and follow up with the Operating Businesses to ensure that corrective measures are taken. The Vice President, Internal Audit, with the assistance of the Internal Audit Department staff, the AGC DPS, and the Operating Businesses, will determine the appropriate scope of the audit program for BCRs to address systems and processes that must adhere to these BCRs.
- Results of the BCRs compliance audits will be communicated to the AGC DPS, who, in turn, will inform the UTC Vice President, Secretary and Associate General Counsel, UTC F&S, and the Privacy Advisory Committee. The UTC Vice President, Secretary and Associate General Counsel will communicate materials audit findings related to the BCRs to the Board of Directors of UTC Corporate Office or a committee of the Board, such as the Audit Committee. Competent Data Protection Authorities in the EEA and Switzerland, 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:

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

Personnel who are direct UTC employees can address their requests and complaints to their local Human Resources representative. All Personnel, including employees, may contact their Local, Regional, or Global Ethics and Compliance Officer (“ECO”), the Ombudsman Program, or the Privacy Office. These resources can be contacted as follows:

Local HR	Contact using your regular internal channels
ECOs	http://ethics.utc.com/Pages/Global%20Ethics%20and%20Compliance%20Officers.aspx
Ombudsman	<p>Internet: Ombudsman.confidential.utc.com</p> <p>Telephone: From within the U.S., Canada and Puerto Rico, call 800.871.9065. When calling from outside the U.S., you must first dial the pertinent AT&T Direct access code found here. Listen for a prompt (voice or tone), and then dial the toll-free number for an Ombudsman.</p> <p>Mail: United Technologies Corporation, Attention: Ombudsman Program 10 Farm Springs Road, 10FS-2 Farmington, CT 06032-2526 USA</p>
Privacy Office	privacy.compliance@utc.com

Complaints submitted to local HR, ECOs, or the Privacy Office: these complaints will be addressed by the group (HR, ECO, or Privacy Office) that has received them, with assistance from the appropriate Privacy Professional or the AGC DPS (or designee) where needed.

Privacy complaints submitted to the Ombudsman Program: 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 the Ombudsman Program or the Privacy Office, which can be reached as follows:

Ombudsman	<p>Internet: Ombudsman.confidential.utc.com</p> <p>Telephone: From within the U.S., Canada and Puerto Rico, call 800.871.9065. When calling from outside the U.S., you must first dial the</p>
-----------	--

	<p>pertinent AT&T Direct access code found here. Listen for a prompt (voice or tone), and then dial the toll-free number for an Ombudsman.</p> <p>Mail: United Technologies Corporation, Attention: Ombudsman Program 10 Farm Springs Road, 10FS-2 Farmington, CT 06032-2526 USA</p>
Privacy Office	privacy.compliance@utc.com

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

c) Additional information about complaint handling

Complaints and audit results revealing structural shortcomings globally will be addressed by AGC DPS through the PAC in order to ensure a global resolution in cooperation with UTC F&S and the local Privacy Professionals.

Any time a complaint cannot be resolved to the complainant’s satisfaction, local HR, the ECO, or the Privacy Professional will report the issue to the AGC DPS. The AGC DPS, in turn, will inform UTC F&S of every complaint that cannot be resolved through the available complaint handling procedures.

UTC will endeavor to provide an initial response within five working days of receiving the request/complaint. Depending on the complexity and scope of the request/complaint, this period may be longer, but should not exceed one month.

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

6. Enforcement Rights of Individuals and Guarantees: Individuals shall have the benefit of the 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 UTC F&S in this Section.

For alleged breaches of these BCRs, Individuals who are residents of the European Union, the United Kingdom or Switzerland, may:

- file a complaint with the data protection authority in the EU Member State of the Individual’s habitual residence, place of work or place of the alleged infringement, at the Individual’s choice; or
- bring an action before a competent court in the EU, 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.

All Individuals who otherwise have rights under these BCRs, including Individuals who are not residents of the European Union, the United Kingdom or Switzerland, have recourse to the statutory redress procedures provided under their applicable national law.

With assistance from the UTC Corporate Office, UTC F&S shall be responsible for ensuring that actions are taken (1) to remedy a breach committed by the UTC 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 damages resulting from the breach of the BCRs by the Corporate Office and/or an Operating Business outside the EEA and Switzerland, unless the relevant Operating Business has already paid the compensation or complied with the order.

Where Individuals can demonstrate that they have suffered damage, then it shall be for UTC F&S, in cooperation with the UTC Corporate Office, to prove that the Corporate office and the Operating Business concerned was not in breach of its obligations under these BCRs. Where such proof can be provided, UTC F&S may discharge itself of any responsibility under the BCRs.

The UTC Corporate Office, shall be responsible for ensuring that actions are taken to remedy a breach committed by Operating Businesses outside of the EEA and Switzerland in respect of Personal Information not originating directly or indirectly from the European Economic Area or Switzerland.

For countries other than the EEA Members States and Switzerland, 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 Data Protection Authorities:** Operating Businesses shall provide any necessary assistance reasonably required by competent data protection authorities in connection with their enquiries and verifications in relation to the BCRs, including providing the results of audits upon request.

UTC shall abide by the decisions of competent EEA/Swiss data protection authorities that are final, *i.e.*, decisions against which no further appeal is possible or decisions which UTC decides not to appeal. UTC accepts that its compliance with the BCRs may be audited by competent data protection authorities in compliance with applicable laws.

- 8. Modification to these BCRs:** UTC F&S shall promptly notify the Belgian Data Protection 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, UTC F&S

shall notify the Belgian Data Protection Authority of all changes that occurred in the previous year.

UTC F&S 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, or EEA/Swiss data protection authorities, upon request. In any event, the UTC F&S shall provide the Belgian Data Protection Authority with a copy of an up-to-date list of all Operating Businesses that have executed a Corporate Rules Agreement not less than once per year.

UTC agrees that it shall not rely upon these BCRs to transfer Individuals' Personal Information to other members of the UTC group until such time as the relevant group members have executed the Intra-Group Agreement and can comply with it.

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

EXHIBIT A - DEFINITIONS

“Business Unit” means UTC’s major segment, which may change from time to time, and currently consistent of Climate, Controls & Security, Otis, Pratt & Whitney, UTC Aerospace Space, UTC Research Center, and the UTC Corporate Office.

“CCS” refers to UTC’s Climate, Controls & Security business unit.

“Corporate Office” refers to the company’s corporate headquarters in the U.S. at 10 Farm Springs Road, Farmington, CT 06032 USA.

“Data Breach” means unauthorized acquisition or use of unencrypted Personal Information, or encrypted Personal Information if there is a compromise of its confidential process or key, that is capable of compromising the security, confidentiality, or integrity of the Personal Information that creates a substantial risk of harm to one or more individuals. The risk of harm includes the possibility of identity theft, potential for embarrassment, release of private information, or other adverse impact. A good faith but unauthorized acquisition of Personal Information by UTC or its Personnel or Service Provider for lawful purposes is not a Data Breach of security unless the Personal Information is used in an unauthorized manner or is subject to further unauthorized disclosure.

“Individuals” means natural persons that are Personnel, UTC customers or suppliers, and consumers of UTC products and services.

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

“Personal Information” means information relating to an identified or identifiable natural person. This is any information relating to a natural person, identified or identifiable, directly or indirectly, in particular by reference to an identifier, such as an identification number, name or one or more factors specific to the person’s physical, physiological, mental, economic, cultural or social identity. Whether an Individual is identifiable depends on the means reasonably likely to be used by UTC or another person to identify the Individual concerned. Where these measures are not reasonably likely to be used for identification is impossible, the data concerned are anonymous and not covered by these BCRs. The term includes Sensitive Personal Information. Personal Information includes information collected, processed, and/or transferred regardless of the medium, including but not limited to hard copy, electronic, video recording, and audio recording.

“Personnel” means UTC employees, including UTC directors and officers, and temporary employees, contractors, leased labor and contract laborers retained by UTC.

“Process” means any operation or set of operations that is performed upon 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 and means information relating to an identified or identifiable person that involves: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health; sexual preference; sex life; or the commission or alleged commission of any crime and possible penalties.

“Service Provider” means any entity or person who/that Processes, or otherwise is permitted access to Personal Information Processed by UTC through its provision of services directly to UTC.

“Third Party” is any individual or entity, other than the UTC Corporate Office and Operating Businesses that executed a Corporate Rules Agreement and their Personnel, and Service Providers.

“UTC” means UTC’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 “UTC Principal”) entrusts a project to another bound Operating Business (hereafter: the “UTC Processor”) that involves the processing of covered Personal Data. To the extent that the project involves a Work Order between UTC Principal and UTC 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 UTC BCRs for the protection of personal information.”

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

1. UTC Principal and UTC Processor agree to remain bound by the UTC 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, UTC Processor will process Personal Information on behalf of UTC Principal.
3. Obligations of UTC Principal:
 - 3.1. UTC Principal shall provide UTC 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 UTC Processor to meet its obligations under these clauses and the UTC BCRs. In particular, UTC Principal’s instructions may govern the use of sub-contractors, the disclosure of Personal Information and other obligations of UTC Processor.
 - 3.2. UTC Principal shall inform UTC 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 UTC Processor under these clauses, and provide instructions on how UTC Processor should comply with such amendments.
4. Obligations of the UTC Processor
 - 4.1. UTC Processor shall Process Personal Information in accordance with the instructions of UTC Principal as set forth in the Work Order and as communicated in writing. UTC Processor shall not carry out Processing of relevant Personal Information for any other purpose or in any other manner.
 - 4.2. UTC Processor shall comply with all provisions of the UTC BCRs and in particular with Section D.1.e.

- 4.3. UTC 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 UTC Principal.
- 4.4. Where, in accordance with the UTC BCRs (Section D.1.f.), UTC 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, UTC Processor shall notify UTC 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 UTC Principal with respect to such disclosures.
- 4.5. UTC Processor shall notify UTC 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 UTC Principal in responding to such communications. In addition, UTC Processor shall provide any and all assistance required by UTC 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. UTC 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 UTC Principal. UTC 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 UTC Processor under these clauses. UTC Processor must comply with UTC BCRs Section D.1.f.
- 4.7. UTC 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 material adverse effect on UTC Processor's compliance with these clauses or in the event UTC Processor otherwise cannot comply with these clauses, UTC Processor shall notify UTC Principal within fifteen (15) business days and UTC Principal shall be entitled to terminate the Work Order with immediate effect.
- 4.8. UTC Processor agrees that UTC Principal may request that UTC Processor's compliance with these clauses is audited in accordance with UTC BCRs Section D.4. In particular, UTC Processor shall make available to UTC Principal all information necessary to demonstrate its compliance with these obligations and submit to audits, including inspections, conducted by UTC principal or an auditor mandated by UTC Principal.
- 4.9. UTC Processor shall ensure that any person Processing Personal Information under the authority of UTC Processor is subject to suitable duties of confidentiality.

- 4.10. UTC Processor shall assist UTC Principal in complying with its obligations under applicable data protection laws, including in completing data protection impact assessments, where applicable.
 - 4.11. UTC Processor shall notify UTC 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 UTC in doing the same where required. UTC or the appropriate Operating Business will coordinate with UTC Principal and UTC Processor regarding the appropriate investigation and remediation. UTC Processor shall also assist UTC Principal as may be necessary to fulfil UTC Principal's obligation to notify a government authority or affected individuals about the data breach.
5. In the event of the termination of the Work Order, UTC Processor shall send to UTC Principal all relevant Personal Information held by UTC Processor, together with all copies in any media of such data or destroy the same, unless UTC 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 UTC principal of any such obligation.
 6. These clauses shall be governed by and construed in accordance with the laws of the country in which UTC Principal is established. Without prejudice to UTC BCRs Section D.6, each party to these clauses irrevocably submits to the exclusive jurisdiction of the country of UTC 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 UTC Principal and UTC Processor and their respective successors and assigns.