EU-U.S. and Swiss-U.S. Privacy Shield Data Protection Plan

Document Number	Revision	Revision Release Date
D950-11106-32	Rev C	November 1, 2021

CONTENT OWNER: Boeing Global Privacy Office

All future revisions to this document shall be approved by the content owner prior to release.

Abstract

This document describes participation in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks by The Boeing Company, and has been approved by the Deputy Chief Privacy Officer.

This document is made available on the Privacy Shield web site, and is available to all Employees on the Boeing internal network.

Table of Contents

1 Introduction

1.1 Purpose

In order to fulfill the European Union requirement that personal information may only be transferred to countries which have an adequate level of data protection, whether by reason of their domestic law or the international commitments they have entered into, The Boeing Company (Boeing) complies with the EU-U.S. and the Swiss-U.S. Privacy Shield Frameworks (Privacy Shield) as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom, or Switzerland to the U.S.in reliance on Privacy Shield. Boeing has certified to the Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about Privacy Shield and to view our certification, please visit https://www.privacyshield.gov/.

Boeing takes other actions in order to comply with the data protection laws in those countries, and where country specific data protection, privacy or security plans are required, those plans are submitted to the appropriate Data Protection Authorities and entered into the Chief Privacy Officer's Registry of Privacy and Data Protection Plans, as is this plan. This plan comprises the Privacy Shield Policy Statement of Boeing.

1.2 Authority and Scope

This plan describes the special controls for personal information about individuals residing in the EU/EEA, Switzerland, and the UK (hereafter referred to as Europe), that is transferred to the U.S. in compliance with applicable laws and regulations, and is required by Boeing policy PRO-98 (this is an internal Boeing document for employees). This document pertains to Boeing enterprise-wide and its wholly owned subsidiaries worldwide, including Continental Graphics Corporation, Aviall, and Boeing Digital Solutions, Inc. doing business as Jeppesen Sanderson.

1.3 Boeing Privacy Framework

The legal frameworks in which personal data is processed vary from jurisdiction to jurisdiction. To address the wide range of privacy principles specified within various jurisdictions, Boeing has adopted the Generally Accepted Privacy Principles (GAPP) as an overall framework. These principles were developed under a joint effort of the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) through the AICPA/CICA Privacy Task Force and can be mapped to privacy principles used around the globe. The CICA has not yet provided a mapping between the GAPP, the principles of the GDPR, or the Privacy Shield Principles; the Boeing Global Privacy Office implements the mapping as follows:

Generally Accepted Privacy Principles	U.S./EU Privacy Shield Principles	General Data Protection Regulation
Notice: How do you provide notice about privacy policies and procedures and identify the purpose for which personal information is collected, used, retained, and disclosed?	1. Notice	1(a) Lawfulness, Fairness and Transparency 1(b) Purpose Limitation
Choice and Consent: How do you provide the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information?	2. Choice	1(a) Lawfulness, Fairness and Transparency
Collection: How do you assure that you collect personal information only for the purposes identified in the notices?	7. Recourse, enforcement and liability	1(a) Lawfulness, Fairness and Transparency 1(c) Data Minimisation
Use and Retention: How do you limit the use of personal information to the purpose identified in the notice and for which the individual has provided implicit or explicit consent?	5. Data integrity and purpose limitation	1(b) Purpose Limitation 1(e) Storage Limitation 2 Accountability
Access: How do you provide individuals with access to their personal information for review and update?	6. Access	1(a) Lawfulness, Fairness and Transparency
Disclosure to Third Parties: How do you control the use of personal data by third parties?	3. Accountability for onward transfer	1(a) Lawfulness, Fairness and Transparency 1(f) Integrity and Confidentiality
Security for Privacy: How do you protect personal information against unauthorized access or use?	4. Security	1(f) Integrity and Confidentiality
Quality: How do you maintain accurate, complete, and relevant personal information for the purposes identified in the notice?	5. Data Integrity and purpose limitation	1(d) Accuracy 1(e) Storage Limitation 1(f) Integrity and Confidentiality 2 Accountability
Monitoring and Enforcement: How do you monitor compliance with your privacy policies and procedures and what procedures do you have to address privacy-related inquiries and disputes?	7. Recourse, enforcement and liability	1(a) Lawfulness, Fairness and Transparency 2 Accountability

2 Participation

In light of the 2020 European Court of Justice decision (often referred to as Schrems II), Boeing will continue to honor the commitments that we have made to the Dept. of Commerce, to our employees and to our customers when we certified under Privacy Shield and with this recertification. To the extent that Privacy Shield participation is no longer sufficient for meeting our on-going regulatory compliance needs, the company will rely on the SCC-based agreements that we have in place, or will avail itself of the other mechanisms for compliance with data protection regulations that were previously fulfilled by participation in the Privacy Shield Program

Participation in Privacy Shield entails the implementation of the 7 Privacy Shield Principles (and the 15 Supplementary Principles) and annual confirmation to the Department of Commerce that Boeing has implemented the requirements of the framework.

Initially, key actions in implementation of the framework were the identification of the business processes that implement the requirements of the framework, the provision of appropriate guidance and tools for implementation and providing the appropriate notice to the individuals whose personal information was transferred to the United States under the auspices of the framework. This was accomplished during the initial self-certification in 2016.

In subsequent years, implementation entails the maintenance of those principles in the business processes of Boeing, the annual verification of continued implementation, responding to inquiries or complaints, and re-certification.

Boeing participation in Privacy Shield is with respect to employee data in the context of the employment relationship, and to process customer data in the context of provisions of service. The collection of the information and its processing prior to transfer will have been subject to the national laws of the European country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected. The Privacy Shield Principles are relevant only when individually identified or identifiable records are transferred or accessed.

In any circumstances where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work. This includes cases where the alleged mishandling of their personal information is the responsibility of the U.S. organization that has received the information from the employer and thus involves an alleged non-compliance with the Privacy Shield Principles. Boeing has committed to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases and with regard to Swiss employees, with the Swiss Federal Data Protection and Information Commissioner.

Although the Privacy Shield frameworks allow for binding arbitration in some cases, when Boeing uses Privacy Shield for HR data, Boeing does not provide for binding arbitration in its implementation of the Frameworks. However, Boeing still pays the International Centre for Dispute Resolution-American Arbitration Association a fee to cover arbitration costs. To facilitate arbitration in regards to Customer data, the Judicial Arbitration and Mediation Services (JAMS) Alternative Dispute Resolution (ADR) is Boeing's Dispute Resolution provider under the EU-U.S. Privacy Shield or the Swiss-U.S. Privacy Shield Frameworks. For additional information, access the JAMS website at https://www.jamsadr.com/eu-us-privacy-shield. Individuals have the possibility, under certain circumstances, to invoke binding arbitration for complaints regarding Privacy Shield compliance not resolved by any of the above Privacy Shield mechanisms. Access additional information on binding arbitration at Privacy Shield Annex 1.

Boeing is also subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission with regard to the Framework.

3 Policy

Joining the Privacy Shield Framework means that Boeing, its wholly owned subsidiaries follow the 7 Privacy Shield Principles (and the 15 Supplementary Principles) with respect to all personal data of individuals transferred to the U.S. from the countries listed in the self-certification. All organizations covered by this filing must comply with the following principles when handling personal information transferred to the U.S. under this framework.

3.1 Notice

3.1.1 An organization must inform individuals about:

i. its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,

ii. the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,

iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield,

iv. the purposes for which it collects and uses personal information about them,

v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,

vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,

vii. the right of individuals to access their personal data,

viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,

ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is:

1. the panel established by DPAs,
2. an alternative dispute resolution provider based in the EU, or
3. an alternative dispute resolution provider based in the United States,

x. being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body,

xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,

xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and

xiii. its liability in cases of onward transfers to third parties.

3.1.2 This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

3.2 Choice

3.2.1 An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.

3.2.2 By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.

3.2.3 For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3.3 Accountability for Onward Transfer

3.3.1 To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.

3.3.2 To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

3.4 Security

3.4.1 Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

3.5 Data Integrity and Purpose Limitation

3.5.1 Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently

authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.

3.5.2 Information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of 3.5.1. This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Organizations should take reasonable and appropriate measures in complying with this provision.

3.6 Access

3.6.1 Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

3.7 Recourse, Enforcement and Liability

3.7.1 Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:

i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;

ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and

iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

3.7.2 Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.

3.7.3 Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.

3.7.4 In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event-giving rise to the damage.

3.7.5 When an organization becomes subject to an FTC or court order based on non-compliance, the organization shall make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

3.8 Supplementary Principles

3.8.1 To the extent that they are relevant, the Supplementary Principles must also be applied to the processing employee data, or to the Boeing Privacy Shield Framework. Some principles, such as the Journalistic Exceptions, will not pertain to processing of employee data by Boeing. Some principles, such as Human Resources Data, will always pertain. Some principles, like Sensitive Data, will pertain to specific data (such as the processing of Religious preference for German employees) and some principles, such as Self-Certification and Verification, will pertain only to specific organizations with Boeing. In any processing of employee data, the Supplementary Principles will be reviewed by the Global Privacy Office to determine if they apply and in what manner.

4 Responsibilities

The Corporate Officer designated as responsible for privacy is the Executive Vice President and General Counsel. Corporate policy POL-1, “Delegation of Authority to Authorize Business Transactions and Agreements, and to Commit Company Resources”, reflects this assignment. Through corporate procedure PRO 98, “Personal Information Protection Practices”, the Executive Vice President has designed the Chief Privacy Officer and the Deputy Chief Privacy Officer as responsible for oversight of data protection and privacy policy, and through the Deputy Chief Privacy Officer’s approval of this plan, the following responsibilities with regard to the Company’s participation in the Privacy Shield Framework are designated to the appropriate company organizations.

4.1 Global Privacy Office (GPO)

The GPO will perform an annual verification required prior to re-certification to the Department of Commerce. The GPO will also follow up on any deficiencies or opportunities for improvement discovered during the verification. The GPO will maintain the records of this verification and respond to any inquiries or complaints that arise out of participation in the Privacy Shield Framework. The GPO will maintain the training materials used for all individuals who access the HR data of European employees, and will also approve any changes to Notices provided to European employees. The GPO is responsible for the Recourse, Enforcement and Liability, including the determination of how other principles, including the Supplementary Principles, pertain to processing European employee’s personal data and to the implementation of the principles at wholly owned subsidiaries.

4.2 Information Security (IS)

IS will implement technical controls for information systems that are sufficient for the Security principle of the Privacy Shield Framework.

4.3 Security and Fire Protection (S&FP)

S&FP will implement security controls for information systems that are sufficient for the Security principle of the Privacy Shield Framework.

4.4 Human Resources Organizations

Human Resources organizations will provide and maintain business processes that implement the Notice, Choice, Data Integrity and Purpose Limitation and Access principles of the Privacy Shield Frameworks. Retention of personal data will be managed in accordance with PRO-251Boeing Records and Information Management (RIM) Program.

4.5 All Organizations Using Personal Information

All organizations using personal information will maintain business processes that implement the Data Integrity and Purpose Limitation and Access principles of the Privacy Shield Framework. Retention of personal data will be managed in accordance with PRO-251 Boeing Records and Information Management (RIM) Program.

5 Notices

Notice is provided during recruiting and hiring processes, and upon customer interaction, while additional notice will be provided if additional personal information is required or additional uses of data are necessary. These notices will be updated from time to time. Current employee notices are available on the internal GPO web site; customer notices are available on the Boeing web site.

5.1 HR Data

During recruiting and hiring processes, a notice is provided to address personal data collected and used in the vetting, selection and offer activities and subsequently retained for accountability. This notice is available here: https://www.boeing.com/careers/privacy-statement.page.

A general privacy notice, such as the one below, will be provided at time of hire, and is made available to all Employees on the internal GPO web site.

Boeing Employee Privacy Notice

This Notice describes the privacy and data protection practices of The Boeing Company and its subsidiaries around the globe (collectively "Boeing" or the "Company") with respect to the processing of Personal Information about employees, former employees, contingent workers and others for employment-related purposes.

Whenever you see the following terms in this notice, they have the meaning as defined below:

- "Personal Information" means any information about an individual, including information that can be used to identify, contact or locate an individual.
- "Processing" means any action we may take related to your personal information, including collection, use, disclosure, handling, storage, transmission, protection, modification, or disposal.
- "Special Categories of Information" means Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, or data concerning an individual's sex life or sexual orientation.

This notice does not replace other notices or consents provided by Boeing to job applicants, employees, contingent workers or others in accordance with national and local laws and regulations. In the event of any conflict between notices or consents required by local law and this notice, the notices or consents required by local law will prevail.

Our Approach: At Boeing, our approach to privacy begins with our enduring values. Consistent with our tradition of practicing high ethical standards and acting with integrity and fairness in everything we do, we have demonstrated our commitment to privacy by establishing a global privacy program to support the protection of Personal Information and enable compliance with applicable privacy laws around the world. Governance for our program relies on two key policies which provide requirements and responsibilities for privacy and security: 1) PRO-98, "Personal Information Protection & Privacy" and 2) PRO-2227, "Information Protection". Additional requirements, guidance and related policies can be found on the Global Privacy Office Website (https://globalprivacy.web.boeing.com). Your careful attention to Boeing's privacy and security practices will help maintain your privacy, and respect and protect the privacy of others.

How We Obtain Personal Data: We obtain Personal Information through fair and lawful means. In many cases, we obtain your Personal Information directly from you or our interactions with you, such as when you complete an application form or enter information about yourself into our systems. In other cases, we develop Personal Information through your interactions with us, such as through your use of Company equipment, systems and networks. Finally, some of the Personal Data we obtain may come from other sources, such as your manager, or in some cases, (with your prior written consent, where required by law) external sources, such as references, background checks, or vendors.

Types of Personal Information we process:

In order to establish, maintain and fulfill our obligations regarding the employment relationship with you, Boeing collects and processes a wide range of Personal Information, including but not limited to the following:

- contact information (e.g., name, home and business addresses, telephone numbers, e-mail addresses, emergency contact information)
- identity and demographic information (e.g., date of birth, marital status, social security or other national identification number, gender, preferred language, birth place, nationality, citizenship, age, race)
- employment, performance, compensation and benefits information (e.g., hire date, adjusted service date, BEMSID, job title, position/grade, ability to work in a particular location, export status, security clearance information, attendance, business unit, supervisor, site, union membership, objectives, projects, performance reviews and leadership ratings, salary, retirement, information about your family or dependents)
- education and training (e.g., education level, field and institution; competency assessments; professional licenses and certifications; training course completions)
- prior employers and employment history (e.g., employers in related industries, government employment, veteran status, references, letters of recommendation, resumes, job application data)
- driver's license number, vehicle license plate number
- financial information (e.g., tax numbers, bank account numbers, personal or Company credit card numbers)
- safety or health-related information (e.g., work restrictions, accommodations, safety incident reports, industrial hygiene exposure and monitoring information)
- agreements that you enter into with the Company
- computer or facilities access and authentication information (e.g., identification codes, passwords), and to the extent permitted by law, monitoring information about your usage of the Company's network, systems, applications and Company provided resources (e.g., computers, phones, and mobile devices)
- photographs and other visual images of you

Processing of Special Categories of Information: We do not process Special Categories of Information except under limited circumstances where permitted or required by law (e.g., collecting religion in Germany where required for taxation purposes, or race/ethnic origin to comply with Equal Employment Opportunity requirements in the U.S.), or where you have otherwise explicitly consented. We will always obtain your explicit consent before Processing Special Categories of Data unless consent is not required by law, for example where the information is required to protect your vital interests or those of a third person and where you are not able to provide consent. If we are Processing Special Categories of data based on your consent, you have the right to withdraw that consent at any time.

Why We Process Personal Information: In most cases, the information processed about you is required by law, is necessary to establish and maintain our employment relationship with you (e.g., to fulfill the conditions of your employment contract), or for Boeing's legitimate business interests related to our employment relationship with you. In other cases, such as maintaining optional benefits programs or participation in optional activities (e.g., wellness activities or advocacy campaigns), Boeing will notify you of your options regarding your participation and the use of your personal data. Boeing will not engage in any adverse actions against you should you choose not to participate in such optional uses of Personal Information. Boeing Processes your Personal Information for a wide range of purposes related to the employment relationship, including but not limited to:

- staffing (e.g., headcount planning, recruitment, termination, succession planning)
- conducting background checks (as permitted by applicable laws) or conflict of interest screening and reporting

- compensation, payroll, and benefit planning and administration (e.g., salary, tax withholding, tax equalization, awards, insurance and pension)
- performance management, workforce development, talent management, education, training and certification
- work shift scheduling, organizational planning and development, and workforce management
- budget planning and administration
- problem resolution (e.g., internal reviews, grievances), investigations, auditing, compliance, risk management and security purposes
- authorizing, granting, administering, monitoring and terminating access to or use of company systems, facilities, records, property and infrastructure
- business travel (e.g., limousines, commercial flights, company aviation services, hotels, rental cars)
- expense management (e.g., corporate card, expense reimbursement processing, procurement)
- project management
- employee communications
- administration of employee enrollment and participation in activities and programs offered to eligible employees (e.g., matching donations to non-profit organizations, political action committee contributions, wellness activities)
- safety incident and work-related injury and illness reporting
- monitoring and surveillance for industrial hygiene, public health and safety
- legal proceedings and government investigations, including preservation of relevant data
- as required or expressly authorized by laws or regulations

Some of the personal information Boeing maintains will be kept in paper files, while other data will be included in computerized files and databases. In either case, the information will be made available for the purposes mentioned above and on a business-need-to-know basis, to responsible management, human resources, accounting, security, and other corporate staff, and to third parties providing services under contract to Boeing, such as payroll processors. Certain information will also be reported to government authorities, for example as required by law for tax or other purposes. Personal information may also be released to external parties as required by labor legislation or agreements, or by legal process, as well as to parties you authorize Boeing to release your information to.

Cross-Border Data Transfers: In addition to personnel and payroll files maintained at your place of employment, some information concerning you may be processed for the purposes mentioned above by The Boeing Company and its subsidiaries in the United States (U.S.) and in other countries around the globe. As a global company, we can achieve important business efficiencies (e.g., operating as “One Boeing”) by consolidating information about our employees, and other individuals about whom the company has employment related (or human resources) Personal Information, in centralized databases and systems located at our facilities in the U.S. or with subsidiaries or third parties who host applications for us. The primary company system of record for human resources data is located in the U.S. This system also shares Personal Information with other systems and databases hosted by or on behalf of our company, however, these other systems and databases will only Process Personal Information in accordance with, and as permitted by applicable laws, including having a legal basis to transfer information to another jurisdiction when required.

In addition to legal provisions such as statutory compliance, fulfillment of contract and treaty compliance, Personal Information transferred to the U.S. from the EU and Switzerland will be protected according the commitment of The Boeing Company and its subsidiaries to principles of the EU-U.S. (and Swiss-U.S.) Privacy Shield Framework (https://www.privacyshield.gov/list). This protection extends to the service providers who process your data on Boeing’s behalf, for which Boeing is responsible. Boeing is subject to the investigatory and enforcement powers of the Federal Trade Commission with regard to the Framework. Complete information on Boeing’s participation in the EU-U.S. Privacy Shield Framework can be found in the EU-U.S. Privacy Shield Data Protection Plan on the Global Privacy Office web page (https://globalprivacy.web.boeing.com).

Data Retention and Disposal: We retain your Personal Information for as long as it is needed to fulfill its intended use and to comply with applicable laws. The required period of retention varies depending the type of information and the laws in your location. The specific retention period for business records is set forth in company retention schedules in accordance with Company Records and Information Management requirements. When no longer needed, we either anonymize or dispose of your Personal Information using Company approved standard methods, which have been developed to prevent loss, theft, misuse or unauthorized access after disposal.

Automated Decision Making: While we do perform Processing using automated means, including analytics, your Personal Information is not subject to any purely automated decision making with a legal or similarly significant impact.

How to Exercise Your Rights: In accordance with the data protection laws where you live, you may have a right to access and correct the information the Company maintains about you. In many cases, we will make available self-help tools to enable you to access or edit your Personal Data. In other cases, you may exercise these rights by using our rights exercise portal (https://boeing.com/privacy/rightsexerciseportal). In certain instances, you may also have the right to have your Personal Information erased (e.g., when the data is no longer needed for the purposes of collection or when you have withdrawn your consent for optional Processing), to restrict Processing of your data, or to object to Processing. Exercise of these rights is facilitated by our rights exercise portal.

California Employees: The California Consumer Privacy Act ("CCPA") provides California employees and contingent workers with specific privacy rights. Employees and workers are entitled to receive notice about the categories of personal information Boeing collects about them and how that information is used, as described throughout this notice. Please contact the Boeing Global Privacy office with inquiries, questions, or requests regarding Boeing's processing of your personal information. Boeing does not sell your personal information.

Contact Us: If you have questions about Boeing's use of your personal information, or wish to file a complaint about it, please contact the Boeing Global Privacy Office using any of the following methods:

- Submit your questions and requests online using the Boeing Privacy Rights Exercise Portal at https://boeing.com/privacy/rightsexerciseportal
  - Call the Global Privacy Office Hotline at +1 (206) 544-2406 or toll-free from within the U.S. at +1 (877) 544-2407
  - Submit your comments or questions to the Global Privacy Office e-mail account at: globalprivacy@boeing.com
  - Writing us at:

    Boeing Global Privacy Office
    Mail Code 45-27
    PO Box 3707
    Seattle, WA 98124-2207
    USA

You may also refer issues to the Privacy or Data Protection/Supervisory Authority where you live: https://www.boeing.com/privacy/authorities.html

Effective Date: November 1, 2021

5.2 Customer Data

The general customer privacy notice is the Boeing Privacy and Cookie Statement, which is available here: https://www.boeing.com/privacy-and-cookie-policy.page

Boeing Digital Solutions, Inc., doing business as Jeppesen, a wholly-owned subsidiary, continues to refer to their own customer privacy shield notice to maintain brand recognition. Examples include:

- https://support.jeppesen.com/privacy
- https://ww2.jeppesen.com/legal/eu-u-s-and-swiss-u-s-privacy-shield-notice/

Revision Record