



## PANASONIC AVIONICS CORPORATION PRIVACY POLICY

EFFECTIVE DATE: February 25, 2019

Panasonic Avionics Corporation (“PAC,” “we,” “us,” or “our”) values your privacy. In this Privacy Policy (“Policy”), we describe how we collect, use, and disclose information that we obtain about visitors to our website <https://www.panasonic.aero/> (the “Site”) and information about individuals at our corporate customers, as well as our employees, and how we use and disclose that information.

By visiting the Site, you acknowledge that your personal information will be handled as described in this Policy. Your use of our Services, and any dispute over privacy, is subject to this Policy and our Terms of Use, including any applicable limitations on damages and the resolution of disputes. The PAC Terms of Use are incorporated by reference into this Policy.

The information we collect through the Site and certain products available through airlines is controlled by Panasonic Avionics Corporation, which is headquartered in the United States at 26200 Enterprise Way, Lake Forest, CA 92630, USA.

### **The Information We Collect About You**

We collect information about you directly from you and from third parties, as well as automatically through your use of our Services.

***Information We Collect Directly From You through the Site.*** The information we collect from you depends on how you use our Site. To request access to our customer portal, myIFE, you must provide us with your name, your job title and the name of the PAC customer company you work for, your contact information, such as your business email and phone number, and the username and password you would like to use to access the portal. When you contact us through the Site, we will collect your name, email address, and your reasons for contacting us.

***Information We Collect Through Our Corporate Customer Relationships.*** In order to manage our customer relationships with our corporate customers, we collect information about and from our customers’ employees. This information includes names, titles, business email addresses and phone numbers, work location, and information about an employee’s role at the corporate customer (such as the department they work in, products or issues worked on, and other similar information). We use this information to administer our corporate customer contracts and to market our products and services to corporate customers.

***Information We Collect Automatically.*** We automatically collect the following information about your use of our Site through cookies, web beacons, and other technologies: your domain name; your browser type and operating system; web pages you view; links you click; your IP address; the length of time you visit our Site and; and the referring URL, or the webpage that led you to our Site. We may combine this information with other information that we have collected about you, including, where applicable, your user name, name, and other personal information. Please see the section “Cookies and Other Tracking Mechanisms” below for more information.

### **How We Use Your Information**

We use your information, including your personal information, for the following purposes:

- To provide our services, to communicate with you about your use of our Site or services, to respond to your inquiries, and for other customer service purposes.
- To tailor the content and information that we may send or display to you, to offer location customization, and personalized help and instructions, and to otherwise personalize your experiences



while using the Site. For example, if you log in to myIFE, we will display information about products and services purchased by your company.

- For marketing and promotional purposes. For example, we may use your information, such as your email address, to send you news and newsletters, special offers, and promotions, or to otherwise contact you about products or information we think may interest you.
- To better understand how users access and use our Site, both on an aggregated and individualized basis, in order to improve our Site and respond to user desires and preferences, and for other research and analytical purposes.
- To administer surveys and questionnaires.
- To administer our customer contracts. For example, we will use a customer's employee's contact information to send our invoices or to send service communications to.
- To comply with applicable legal or regulatory obligations, including as part of a judicial proceeding; to respond to a subpoena, warrant, court order, or other legal process; or as part of an investigation or request, whether formal or informal, from law enforcement or a governmental authority.
- To protect the safety, rights, property, or security of PAC, our services, any third party, or the general public; to detect, prevent, or otherwise address fraud, security, or technical issues; to prevent or stop activity that PAC, in its sole discretion, may consider to be, or to pose a risk of being, an illegal, unethical, or legally actionable activity; to use as evidence in litigation; to conduct audits; and to enforce this Policy or our Terms of Use.

### How We Share Your Information

We share your information, including personal information, as follows:

- **Affiliates.** We may disclose the information we collect on the Site or from our customers to our affiliates or subsidiaries for the purposes described in this Policy; however, if we do so, their use and disclosure of your personal information will be subject to this Policy.
- **Service Providers.** We may disclose the information we collect from you to third party vendors, service providers, contractors or agents who perform functions on our behalf.

We also may disclose information in the following circumstances.

- **Business Transfers.** If we are or may be acquired by or merged with another company, if any of our assets are transferred to another company, or as part of a bankruptcy proceeding, we may transfer the information we have collected from you to the other company.
- **In Response to Legal Process.** We also may disclose the information we collect from you in order to comply with the law, a judicial proceeding, court order, or other legal process, such as in response to a court order or a subpoena.
- **To Protect Us and Others.** We also may disclose the information we collect from you where we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of our Terms of Service or this Policy, or as evidence in litigation in which PAC is involved.
- **Aggregate and De-Identified Information.** We may share aggregate or de-identified information about users with third parties for marketing, advertising, research or similar purposes.

### Our Use of Cookies and Other Tracking Mechanisms

We and our third party service providers may use cookies and other tracking mechanisms to track information about your use of our Site. We may combine this information with other personal information we collect from you (and our third party service providers may do so on our behalf).



**Cookies.** Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your web browser for record-keeping purposes. Some cookies allow us to make it easier for you to navigate our Site, while others are used to enable a faster log-in process or to allow us to track your activities at our Site.

**Disabling Cookies.** Most web browsers automatically accept cookies, but if you prefer, you can edit your browser options to block them in the future. The Help portion of the toolbar on most browsers will tell you how to prevent your computer from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Users of our Site who disable cookies may find that some aspects of the Site may not function properly; for example, if you disable cookies, you may not be able to automatically sign in to the Site.

**Clear GIFs, pixel tags and other technologies.** Clear GIFs are tiny graphics with a unique identifier, similar in function to cookies. In contrast to cookies, which are stored on your computer's hard drive, clear GIFs are embedded invisibly on web pages. We may use clear GIFs (a.k.a. web beacons, web bugs or pixel tags), in connection with our Site to, among other things, track the activities of Site visitors, help us manage content, and compile statistics about Site usage. We and our third party service providers also use clear GIFs in HTML emails to our customers, to help us track email response rates, identify when our emails are viewed, and track whether our emails are forwarded.

**Third Party Analytics.** We use automated devices and applications, such as Google Analytics, to evaluate usage of our Site. We also may use other analytic means to evaluate our Site. We use these tools to help us improve our Site, performance, and user experiences. These entities may use cookies and other tracking technologies to perform their services. To learn more about Google's privacy practices, please review the Google Privacy Policy at <https://www.google.com/policies/privacy/>. You can also download the Google Analytics Opt-out Browser Add-on to prevent their data from being used by Google Analytics at <https://tools.google.com/dlpage/gaoptout>.

**Do Not Track.** Currently, our systems do not recognize web browser Do Not Track signals. For more information about Do Not Track signals, please visit [www.allaboutdnt.com](http://www.allaboutdnt.com).

### **Third-Party Links**

Our Site may contain links to third-party websites. Any access to and use of such linked websites is not governed by this Policy, but instead is governed by the privacy policies of those third party websites. We are not responsible for the information practices of such third party websites.

### **Security of My Personal Information**

We have implemented reasonable precautions to protect the information we collect from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. Please be aware that despite our best efforts, no data security measures can guarantee security.

You should take steps to protect against unauthorized access to your password, phone, and computer by, among other things, signing off after using a shared computer, choosing a robust password that nobody else knows or can easily guess, and keeping your log-in and password private. We are not responsible for any lost, stolen, or compromised passwords or for any activity on your account via unauthorized password activity.

### **Access To My Personal Information**

If you have created an account to access myIFE, you may modify the personal information that you have submitted by logging into your account and updating your information. Please note that copies of



information that you have updated, modified or deleted may remain viewable in cached and archived pages of the Services for a period of time.

If you are a resident of the European Union, please see the Information for EU Individuals section below for additional information on accessing your information and other legal rights available to you under European Union law.

### **What Choices Do I Have Regarding Promotional Emails?**

We may send periodic promotional emails to you. You may opt-out of such promotional emails by following the opt-out instructions contained in the email. Please note that it may take up to 10 business days for us to process opt-out requests. If you opt-out of receiving promotional emails, we may still send you emails about your account or any services you have requested or received from us.

### **INFORMATION FOR EU INDIVIDUALS**

Our Policy lays out strict requirements for handling personal data pertaining to customers, prospects, business partners and employees. It meets the requirements of the General Data protection Regulation (GDPR), US-EU Privacy Shield framework, US-Swiss Safe Harbor and ensures compliance with the applicable principles of national and international data protection laws. The policy sets a globally applicable data protection and security standard for our company and regulates the sharing of information between our business units, subsidiaries and affiliates.

As part of the overall compliance effort, and particularly as part of the participation in the US-EU Privacy Shield, we are committed to comply with the Privacy Principles pertaining to (1) Notice, (2) Data Integrity and Purpose Limitation, (3) Choice, (4) Security, (5) Access, (6) Accountability for Onward Transfer, and (7) Recourse, Enforcement and Liability. Detailed explanation of these Principles can be found on the US-EU Privacy Shield website at <https://www.privacyshield.gov> .

Our managers and employees are obligated to adhere to the Panasonic Data Protection Policy and observe all applicable data protection laws and regulations.

**DEFINITIONS.** Throughout this Policy we use the terms “Personal Information“ and “Sensitive Personal Information”. The meaning of those terms may vary depending on the jurisdiction. For the purposes of the Policy the following definitions will apply to those terms:

"Personal Information" means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

"Sensitive Personal Information" means personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information pertaining to the sex life of the individual.

**PRIVACY SHIELD.** Panasonic Avionics Corporation participates in the Privacy Shield framework. Our certification with the Privacy Shield may be verified by accessing the Privacy Shield List at <https://www.privacyshield.gov>.

### **PRIVACY SHIELD PRINCIPLES**

We comply with the seven Privacy Principles established by the Privacy Shield:



1. **NOTICE.** By providing this Policy we inform you about (1) our participation in the Privacy Shield and provide above a link to the Privacy Shield List, (2) the types of personal data we collect and the adherence of all our business units, subsidiaries and affiliates to the Principles, (3) our commitment to treat all personal data received from the EU in reliance on the Privacy Shield in accordance with the Principles, (4) the purposes for which it collects and uses personal information, (5) how to contact us with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints, (6) the type or identity of third parties to which we disclose personal information, and the purposes for which we do so, (7) the right of individuals to access their personal data, (8) the choices and means we offer individuals for limiting the use and disclosure of their personal data, and (9) the independent dispute resolution body designated to address complaints and provide appropriate and free-of-charge recourse, (10) being subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission, the U.S. Department of Transportation or any other U.S. authorized statutory body, (11) your right, under certain conditions, to invoke binding arbitration, (12) our requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and (13) our liability in cases of onward transfers to third parties.

2. **CHOICE.** We offer you the opportunity to choose (opt out) whether your personal information is (1) to be disclosed to a third party or (2) to be used for a purpose that is materially different from the purpose for which it was originally collected or subsequently authorized by you. If this option is not offered to you automatically when the information is collected please contact us at the contact information provided below.

Please note that in some cases it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform tasks on behalf of and under the instructions of the organization. However, we will always enter into a contract with the agent.

For sensitive personal information, we will obtain the affirmative express consent (“opt-in”) from you if such information is to be (1) disclosed to a third party or (2) used for a purpose other than those for which it was originally collected or subsequently authorized by you through the exercise of opt-in choice. In addition, we should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. **ACCOUNTABILITY FOR ONWARD TRANSFER.** To transfer personal information to a third party acting as a controller, we comply with the Notice and Choice Principles. We 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 you and that the recipient will provide the same level of protection as the Principles.

To transfer personal data to a third party acting as an agent, we: (1) transfer such data only for limited and specified purposes; (2) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (3) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the our obligations under the Principles; (4) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and (5) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Privacy Shield organization upon request.

4. **SECURITY.** We have in place reasonable and appropriate measures to protect the Personal Information 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.

5. **DATA INTEGRITY AND PURPOSE LIMITATION.** Our processing of Personal Information is limited to the information that is relevant for the purposes of processing. We do not process Personal Information in a way that is incompatible with the purposes for which it has been collected or subsequently



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

6. **ACCESS.** We will provide you with access to your Personal Information that we hold and you will 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 your privacy in the case in question, or where the rights of persons other than you would be violated.

7. **RECOURSE, ENFORCEMENT, AND LIABILITY.** 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. Therefore, our Policy provides for: (1) readily available independent recourse mechanisms by which your complaints and disputes will be investigated and expeditiously resolved at no cost to you and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide; (2) follow-up procedures for verifying that the attestations and assertions we make about our privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of noncompliance; and (3) obligations to remedy problems arising out of our failure to comply with the Principles and compliance with any sanctions assessed against us.

**PANASONIC RECOURSE MECHANISM.** Any questions or concerns regarding the use or disclosure of personal information should be directed to address listed in the Contact section of this Policy, below. We will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information by reference to the principles contained in this Policy. For complaints that cannot be resolved directly between us and you, we have agreed to participate in the following dispute resolution procedures in the investigation and resolution of complaints to resolve disputes pursuant to the Privacy Shield Principles: (1) for disputes involving employment-related personal information received by us from the EEA, we have agreed to cooperate with the data protection authorities in the EEA and to participate in the dispute resolution procedures of the panel established by the European data protection authorities; (2) for disputes involving all other personal information received by us from the EEA, we have agreed to use International Centre for Dispute Resolution, a division of the American Arbitration Association dispute resolution (“ICDR/AAA”). Individuals who submit a question or concern to us and who do not receive acknowledgment of the inquiry or who think their question or concern has not been satisfactorily addressed should then contact the ICDR/AAA on the Internet (<http://www.icdr.org>), by mail, phone or by fax. The website lists the addresses, phone/fax number for your location. Inquiries by mail or fax should identify Panasonic Avionics Corporation as the company to which a concern or question has been submitted, and include a description of the privacy concern, the name of the individual submitting the inquiry, and whether ICDR/AAA may share the details of the inquiry with us. ICDR/AAA will act as a liaison to our company to resolve these disputes. The dispute resolution process shall be conducted in English. Please note that we are also subject to the jurisdiction of the U.S. Federal Trade Commission and other U.S. government agencies.

## GDPR COMPLIANCE

***When we act as Data Controller:*** If we process your personal information in our capacity as a data controller, the following applies:

We collect, use, and share your personal information where we are satisfied that we have an appropriate legal basis to do this. This may be because:

- Our use of your personal information is necessary to perform a contract or take steps to enter into a contract with you (for example when you choose to subscribe to inflight Wi-Fi services); or



- Our use of your personal information is in our legitimate interest as a commercial organization (for example in order to make improvements to our products and services and to provide you with information you request); you have a right to object to processing as explained in the section below titled Your Legal Rights;
- Our use of your personal information is necessary to comply with a relevant legal or regulatory obligation that we have (for example, where we are required to disclose personal information to a court); or
- Our use of your personal information is in accordance with your consent (for example, when you consent to the receipt of marketing communications is required by local law).

If you would like to find out more about the legal bases on which we process personal information, please contact us using the details below.

**Your Legal Rights.** Subject to certain exemptions, and in some cases dependent upon the processing activity we are undertaking, European Union individuals have certain rights in relation to your personal information:

*Right to access, correct, and delete your personal information:* You have the right to request access to the personal information that we hold about you and:(a) the source of your personal information; (b) the purposes, legal basis and methods of processing; (c) the data controller’s identity; and (d) the entities or categories of entities to whom your personal information may be transferred.

You also have the right to request that we delete your information.

We are not required to comply with your request to erase personal information if the processing of your personal information is necessary for compliance with a legal obligation or for the establishment, exercise, or deference of legal claims.

*Right to restrict the processing of your personal information:* You have the right to restrict the use of your personal information when (i) you contest the accuracy of the data; (ii) the use is unlawful but you do not want us to erase the data; (iii) we no longer need the personal information for the relevant purposes, but we require it for the establishment, exercise, or defense of legal claims; or (iv) you have objected to our personal information use justified on our legitimate interests verification as to whether we have a compelling interest to continue to use your data.

We can continue to use your personal information following a request for restriction, where:

- we have your consent; or
- to establish, exercise or defend legal claims; or
- to protect the rights of another natural or legal person.

*Right to data portability:* To the extent that we process your information (i) based on your consent or under a contract; and (ii) through automated means, you have the right to receive such personal information in a structured, commonly used, machine-readable format, or you can ask to have it transferred directly to another data controller.

*Right to object to the processing of your personal information:* You can object to any processing of your personal information which has our legitimate interests as its legal basis, if you believe your fundamental rights and freedoms outweigh our legitimate interests. If you raise an objection, we have an opportunity to demonstrate that we have compelling legitimate interests which override your rights and freedoms.



*Right to obtain a copy of personal information safeguards used for transfers outside your jurisdiction:* You can ask to obtain a copy of, or reference to, the safeguards under which your personal information is transferred outside of the EEA.

We ask that you please attempt to resolve any issues with us first, although you have a right to contact your supervisory authority as well.

*How to Exercise Your Rights:* If you would like to exercise any of the rights described above, please send us a request [privacy@panasonic.aero](mailto:privacy@panasonic.aero). In your message, please indicate the right you would like to exercise and the information that you would like to access, review, correct, or delete.

We may ask you for additional information to confirm your identity and for security purposes, before disclosing the personal information requested to you. We reserve the right to charge a fee where permitted by law, for instance if your request is manifestly unfounded or excessive.

We may not always be able to fully address your request, for example if it would impact the duty of confidentiality we owe to others, or if we are legally entitled to deal with the request in a different way.

### **EU Data Protection Authorities**

PAC commits to cooperate with EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) and comply with the advice given by such authorities with regard to human resources data transferred from the EU and Switzerland in the context of the employment relationship.

*If we process your data as a Data Processor:* For certain activities where we provide inflight Wi-Fi and entertainment services to our corporate customers, including airlines, we act only on the instruction of those corporate customers. In those situations, the corporate customer is the Data Controller for that purpose. Where we process your data in our capacity as a data processor on behalf of the Data Controller, you may exercise your data subject access rights by contacting your airline directly, or we will forward your request directly to your airline.

### **EU Data Protection Authorities**

PAC commits to cooperate with EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) and comply with the advice given by such authorities with regard to human resources data transferred from the EU and Switzerland in the context of the employment relationship.

**Cross-border Transfer of Information.** PAC generally maintains servers and systems in the United States hosted by third party service providers. We also may subcontract the processing of your data to, or otherwise share your data with, other third parties in the United States or countries other than your country of residence. As a result, where the personal information that we collect through the Site or in connection with providing services to or administering our relationship with a corporate customer is transferred to and processed in the United States or anywhere else outside the European Economic Area (EEA) for the purposes described above, we will take steps to ensure that the information receives the same level of protection as if it remained within the EEA, including entering into data transfer agreements, using the EU Commission approved Standard Contractual Clauses, or by relying on certification schemes such as the EU - US Privacy Shield. You have a right to details of the mechanisms under which your data is transferred outside the EEA. Please see our Privacy Shield Notice or visit [www.privacyshield.gov](http://www.privacyshield.gov) for information about our Privacy Shield practices and certification.



### **Contact Us**

If you have questions about the privacy aspects of our Site or would like to make a complaint, please contact us at [privacy@panasonic.aero](mailto:privacy@panasonic.aero).

### **Changes to this Policy**

This Policy is current as of the Effective Date set forth above. We may change this Policy from time to time, so please be sure to check back periodically. We will post any changes to this Policy on our Site. If we make any changes to this Policy that materially affect our practices with regard to the personal information we have previously collected from you, we will endeavor to provide you with notice in advance of such change by highlighting the change on our Site.