

The privacy and cookie files policy of Polskie Linie Lotnicze LOT S.A.

Last update on [28.10.2021]

GENERAL INFORMATION

This Privacy Policy ("Policy") applies to the personal data of the passengers ("Passengers") of **Polskie Linie Lotnicze LOT S.A.** with its registered office in Warsaw ("PLL LOT" or "we"), and persons for which we provide electronically supplied services through the website www.lot.com ("Website"), and also whose data we process in connection with the use of the mobile application, our social media profiles and as part of other content or online services which we provide (jointly "Users"). The content of the Regulations for the provision of electronically supplied services is available [here](#). The website, our mobile application and social media profiles, as well as other content or services, which we may provide online, are hereinafter jointly referred to as "Services".

The Controller of Users' personal data within the meaning of relevant, applicable provisions on the protection of personal data, including the provisions of the Regulation of the European Parliament and the Council (EU) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation) ("GDPR"), is PLL LOT.

We can be contacted by filling in [contact form](#) or in writing to the address of our registered office: ul. Komitetu Obrony Robotników 43, 02-146 Warszawa.

We have appointed a **data protection officer** – it is a person who can be contacted by Users in all matters concerning the processing of personal data and the use of data processing rights.

The Personal Data Protection Officer can be contacted by e-mail: iod@lot.pl, filling in [contact form](#) or in writing to the address of our registered office: ul. Komitetu Obrony Robotników 43, 02-146 Warszawa.

II. WHAT ARE USERS' RIGHTS?

Subject to the principles set out in Articles 15-18 and Articles 20-21 of the GDPR, Users have at any time the following rights:

- the right to access personal data,
- the right to demand rectification of personal data,
- the right to demand deletion of personal data,
- the right to restrict the processing of personal data,
- the right to transfer personal data – i.e. the right to receive personal data from PLL LOT in a structured, commonly used IT format suitable for machine reading; the right to transfer personal data applies in relation to that data that is processed on the basis of an agreement or consent,
- the right to raise an objection to the processing of personal data – where data is processed on the basis of the legitimate interest of PLL LOT.

Moreover, in the case of processing of personal data on the basis of a consent, Users are **entitled to withdraw the consent** to the processing of data at any time. The withdrawal of consent does not affect the legality of processing which was made on the basis of a consent before its withdrawal.

In order to exercise the above-mentioned rights, one should call the 24-hour Client Service Centre 0 801 703 703 or ticket sales offices or the Data Protection Officer: iod@lot.pl.

Users are also entitled to **lodge a complaint with a supervisory authority** dealing with personal data protection. The leading supervisory authority for PLL LOT is the President of the Personal Data Protection Office.

III. WHICH PERSONAL DATA OF USERS DO WE PROCESS?

We process the following categories of personal data:

- **Technical data:** inter alia type and version of the browser, operating system used by the User, website from which the User was redirected to the Website (URL

address of the redirecting website), and data of the internet service provider or mobile network operator, internet protocol address (IP), cookie files and similar technologies described in more detail in Chapter IX of the Policy, device identifier, MAC physical address, device and browser settings.

- **Analytical data:** inter alia data about usage of the Website, including visited subpages, viewed content, downloaded documents, other undertaken actions, the way of using different functionalities, booking history, agreements concluded with us and services provided by us, and also other interactions with us, our content or our communication, including that provided by external service providers (e.g. Adobe).

- **Data from other sources:** demographic, geographical data, data about interactions with external service providers.

- **Data of the PLL LOT account:** inter alia title, name and surname, gender, cell phone number, e-mail address, correspondence address, card number in the loyalty program, booking history, agreements concluded with us and services provided by us, preferences of the User.

- **Data on contract of carriage:** inter alia date of birth of the Passenger, gender of the Passenger, name and surname of the Passenger, citizenship of the Passenger, country of residence of the Passenger, validity period of the travel document of the Passenger, identifier of the travel document of the Passenger, country of issue of the travel document of the Passenger, type of travel document of the Passenger, name and surname of the Client, citizenship of the Client, phone number of the Client.

- **Data on marketing communication:** inter alia name and surname and contact data (phone number, e-mail address), information on previous bookings, and if the passenger has unfinished bookings – chosen starting and destination airport, information if the flight is in one direction or also return, dates and hours of departure/arrival, number of passengers, chosen type of fare, total fare cost, information if the passenger subscribes to the newsletter, booking type, chosen services, language chosen on the website/in the application.

· **Data related to ensuring safety** inter alia name and surname of the User, address, phone number, IP address, data identifying geographical location, booking and transaction history, credit/debit card data, information on claims and complaints.

The processing of special categories of data (**sensitive data**): In some cases LOT processes special categories of personal data (sensitive data), such as data related to the state of health, for example data on motor disability in the case of Passengers with special needs.

IV. FOR WHAT PURPOSES, ON WHAT BASIS AND HOW LONG DO WE PROCESS PERSONAL DATA?

PLL LOT processes personal data of Users for a number of purposes set out below, based on legal bases indicated below and stores them for the period given below:

Purpose of processing	Categories of processed personal data	Basis for processing of data	Retention period
<p>Operation of the Website and other Services</p> <p>Making available of the Services, including the provision of services available through the Website such as making a booking and enabling the management of the booking (e.g. by choosing additional services),</p>	<p>Technical data</p> <p>Analytical data</p> <p>Data of the PLL LOT account</p>	<p>Performance of the agreement (Art. 6 par. 1 letter b of the GDPR)</p>	<p>for the duration of the agreement or the provision of services</p>

<p>issuing of an electronic air ticket or subscribing for a loyalty program</p>			
<p>Implementation of a carriage contract</p> <p>Undertaking actions before conclusion of the contract, the exercise of rights and obligations resulting from the carriage contract and performance of other services for the Passenger related to air carriage</p>	<p>Data on carriage contract</p>	<p>Performance of the contract (Art. 6 par. 1 letter b of the GDPR)</p>	<p>for the duration of the contract and settlements after its termination</p>
<p>Promotion, advertisement and marketing of our services and the products and services of our partners</p> <p>Adjustment of content in the Services to the interests and preferences of Users, including displaying to Users of personalized content,</p>	<p>Technical data</p> <p>Analytical data</p> <p>Data of the PLL LOT account</p> <p>Data from other sources</p> <p>Data on marketing communication</p>	<p>Legitimate interest (Art. 6 par. 1 letter f of the GDPR), inter alia including raising the attractiveness of the Services, enhancing the effectiveness of our marketing and sales activities through directing</p>	<p>no longer than until objection is raised or consent withdrawn</p>

<p>including communications, promotions, offers, advertisements, recommendations concerning our products and services or promotional actions in the Services and elsewhere (e.g. on websites of our partners – third parties, in social media), and also displaying of our personalized content to the users of our partners - suppliers of websites and social media, and also displaying to Users the content of our partners on the basis of the interests or preferences of Users.</p> <p>Measurement of effectiveness of marketing campaigns, including the settlement of marketing and sales activities.</p>		<p>of personalized content to Users, which may be interested by our offer, analysis of advertising campaigns and creation of more tailored group of recipients, settlements with providers of advertising services</p> <p>Consent (if it is required under applicable provisions) – to the extent indicated in its content</p>	
<p>Marketing communication,</p>	<p>Technical data</p>	<p>Legitimate interest (Art. 6 par. 1 letter</p>	<p>no longer than until consent is</p>

<p>including directing of personalized information concerning our services or products or the services or products of our partners through all distance communication channels, including through e-mail, SMS/MMS, notifications in the browser or the device's operating system or in the application; communication will be created on the basis of the interests and preferences of Users; communication will include inter alia our current offer, information on promotions and services placed on the market, organized events and competitions and special offers, including in the form of our newsletter.</p>	<p>Analytical data Data of the PLL LOT account Data on marketing communication</p>	<p>f of the GDPR), that is conducting the marketing of our products and services, including enhancing the effectiveness of our marketing and sales activities by directing personalized communications to Users whose activity and other data indicate that they may be our offer</p> <p>Consent (if it is required under applicable provisions) – to the extent indicated in its content</p>	<p>revoked or objection raised</p>
<p>Statistical, analytical and reporting, including analyses of Users' activities (including on the basis of profiling), in order to measure traffic in the</p>	<p>Technical data Analytical data</p>	<p>Legitimate interest (Art. 6 par. 1 letter f of the GDPR), i.e. improvement of the quality of services, raising</p>	<p>Until objection is raised</p>

<p>Services and improve or optimize the experience of using the Services, and also reports and alerts related to the functioning of the Services, including with possible errors; statistical analyses and market research (including on the basis of profiling), including analyses of the effectiveness of marketing and promotional activities; satisfaction survey of Users, inter alia on the basis of a customer service satisfaction survey or survey concerning our products and services (including on the basis of profiling).</p>	<p>Data of the PLL LOT account</p> <p>Data on marketing communication</p>	<p>the attractiveness of the Services and adapting them to Users' needs</p>	
<p>Improvement of our products and services (including on the basis of profiling)</p> <p>In particular tests of new functionalities in the Services, correction of errors.</p>	<p>Technical data</p> <p>Analytical data</p>	<p>Legitimate interest (Art. 6 par. 1 letter f of the GDPR), including enhancing the attractiveness of our products and services</p>	

<p>Ensuring safety, including cybersecurity</p> <p>Detection and prevention of threats to the Services, including detection of attack attempts, frauds, abuses.</p>	<p>Technical data</p> <p>Analytical data</p>	<p>Legitimate interest (Art. 6 par. 1 letter f of the GDPR), including ensuring safe use of the Services and protection of servers and IT resources</p>	
<p>Ensuring compliance with legal provisions</p> <p>Including use for accounting, bookkeeping, tax and other purposes, related to the performance of our legal obligations</p>		<p>Performance of obligations resulting from legal provisions (Art. 6 par. 1 letter c of the GDPR)</p>	<p>Until the legal obligation expires, including until the date of approval of the financial report for a given financial year, or no longer than for a period of 5 years from the end of the calendar year, in which tax obligation arose.</p>
<p>User Service, including receiving and considering complaints, grievances and questions, carrying out a passenger complaint procedure in air transport,</p>	<p>Data of the PLL LOT account</p>	<p>Performance of the agreement (e.g. carriage contract) (Art. 6 par. 1 letter b of the GDPR)</p>	<p>Until the expiry of claims under carriage contract or the expiry of the limitation period for claims</p>

<p>communication with Users, including through the Client Service Centre, ticket sales offices, the Website or Services</p>		<p>Performance of obligations resulting from legal provisions (Art. 6 par. 1 letter c of the GDPR)</p> <p>Legitimate interest (Art. 6 par. 1 letter f of the GDPR) consisting in conducting communication with Users, answering questions, resolving amicably contentious issues</p>	
<p>Determination, pursuit or defense against claims, including storing of data for archiving (evidentiary) purposes</p>	<p>Technical data</p> <p>Analytical data</p>	<p>Legitimate interest (Art. 6 par. 1 letter f of the GDPR) i.e. securing information in the event of a legal need to prove facts</p>	<p>Until the expiry of claims</p>
<p>Linking up of devices and browsers or operating systems used</p>	<p>Technical data</p> <p>Analytical data</p>	<p>Legitimate interest (Art. 6 par. 1 letter f of the GDPR)</p>	<p>Until objection is raised</p>

<p>on them as belonging to the same User in order to achieve one or more purposes described above</p>	<p>Data of the PLL LOT account Data on marketing communication</p>	<p>consisting in providing the User with uniform experience when using the Services from different devices</p>	
<p>Combining data coming from different sources (including offline), which were originally collected in contexts other than data collected online in order to achieve one or more purposes described above</p>	<p>Technical data Analytical data Data of the PLL LOT account Data on marketing communication</p>	<p>Legitimate interest (Art. 6 par. 1 letter f of the GDPR) consisting in adjusting the content and communication with the User to the history of the relationship with them</p>	<p>Until the expiry of the retention periods of source data</p>

V. VOLUNTARY NATURE OR OBLIGATION TO PROVIDE DATA

Depending on the purpose of the processing of personal data, their provision may be a condition for the conclusion of an agreement (e.g. in the case of conclusion of a carriage contract) or may be voluntary, but necessary for using our services provided as part of the Services or necessary for User Service, including considering a complaint or grievance.

The provision of personal data for promotional, advertising and marketing purposes is voluntary.

VI. SOURCES OF DATA

In principle, the data which we process we have collected from Users who provided them to us by filling in appropriate forms e.g. during booking or by creating a PLL LOT account. We can also collect Users' data by observing them (e.g. the way of using the Services) or create statistics concerning Users or their profiles. We can also obtain Users' data from our partners, e.g. within the context of marketing or sales activities we obtain data on the effectiveness of the activities of our partners aimed at the promotion or sale of our services, or of our activities addressed at Users (e.g. internet identifiers of Users who have used our services through the services of our partner), and also data which allow us to undertake marketing, advertising activities addressed at Users, who may be interested by our offer (e.g. the demographic, geographical, interests or preferences group to which the User belongs, together with an internet identifier allowing to display them our content).

VII. PROCESSING PASSENGERS' PERSONAL DATA – ADDITIONAL INFORMATION

Due to the necessity of ensuring a safe and lawful journey to our Passengers, we also inform that PLL LOT will process Passengers' personal data in connection with the performance of obligations imposed on PLL LOT under legal provisions. The processing of Passengers' data will take place in particular to:

- fulfil the requirements related to the crossing of a border by the Passenger, inter alia to fulfil immigration, customs and other requirements related to the crossing of the border in destination countries;

- prevent terrorism and other international crimes and to combat them, including to compare Passengers' data to the lists of passengers constituting a threat for aviation security;
- ensure a safe flight to Passengers, and also US safety, in the case of travel between the European Union and the United States.

Detailed rules for the processing of Passengers' personal data travelling between the European Union and the United States have been described in Chapter XII of this Policy.

VIII. HOW LONG DO WE STORE USERS' DATA?

The period of storage of Users' personal data depends on the purpose for which this processing is made. We store personal data for the period necessary to achieve the purposes set out in the Policy, including for the period required by legal provisions or until the expiry of the limitation period for claims. Detailed information has been provided in chapter IV of the Policy. However, we inform that personal data on the travel and bookings of Passengers traveling between the European Union and the United States, referred to as "data concerning the passenger's flight" or "PNR data" (PNR = *Passenger Name Record*) hereinafter as "PNR data", will be stored for the period indicated in chapter XII of this Policy.

IX. TRANSFERRING PERSONAL DATA

PLL LOT may make available Users' personal data to other persons, authorities, institutions and carriers, which in connection with applicable legal provisions, as well as international agreements are authorized to receive such information, or if the transfer of data is necessary to fulfill legitimate purposes pursued by PLL LOT or recipients of data, including inter alia to fulfill immigration, customs and other requirements related to the crossing of a border in destination countries.

PLL LOT may also transfer Users' personal data to their suppliers to whom PLL LOT commissions services related to the processing of personal data e.g. providers of hosting services, providers of analytical, advertising and marketing services, tools used to send marketing communication or entities providing services in the field of administration, maintenance and management of the Website. Such entities will usually process data on the basis of an entrustment agreement concluded with PLL

LOT and only in accordance with PLL LOT's instructions. On the basis of legitimate interest or consent, we may also make available Users' data to our advertising and marketing partners, including providers of analytical and marketing services, which will process them for their purposes as independent controllers.

Where we process statistical data on the User's activity in the PLL LOT profile in the Facebook and Instagram community services, as well as in the case of using pixel or the Facebook plugin on the Website or in the mobile application, there is joint controlling of Users' data between PLL LOT and Facebook Ireland Limited for the needs of creation of aggregated statistics of these Services. The arrangements setting out the scope of joint controlling, including the rules of responsibility for the processing of Users' data can be found on the website: https://www.facebook.com/legal/terms/page_controller_addendum.

According to these rules, Facebook undertakes to take primary responsibility for the processing of Users' data for the needs of statistics and for the fulfillment of other relevant obligations set out in the GDPR.

We may transfer Users' data to our partners, suppliers and subcontractors localized outside the European Economic Area ("EEA"). In such cases we implement specific security measures, making every effort to transfer data to a country considered by the European Commission as providing an adequate level of protection for personal data (the list is available [here](#)) or signing Standard Contractual Clauses approved by the European Commission and, where appropriate, implementing additional contractual, technical and organizational measures (you may receive of copy of such clauses or other security measures, by contacting us in the manner indicated in chapter I of the Policy).

To process payments for your trips and purchases, we may work with third parties that offer payment services. They operate their own privacy policies in terms of the way in which they use your personal data. For transactions acquired in India, the governing law is Indian, including the Indian privacy act.

X PROTECTION OF PERSONAL DATA

We assure that we make every effort to ensure that the processing of Users' personal data takes place with the utmost respect for their privacy and with the utmost care for the safety of the processed personal data. In particular, we assure that we have undertaken all measures provided for by legal provisions to protect data transferred to us, including, in particular:

- we use appropriate technical and organizational measures to ensure the protection of the processed personal data to the extent corresponding to the risk of the violation of rights and freedoms of persons whose data is processed;
- measures referred to in letter a) are implemented both while specifying manners of processing (in the so-called designing phase) and during the processing itself taking into account the level of technical knowledge, the cost of implementation as well as the character, scope, context and purpose of the processing of data;
- we process data respecting the rule of data protection by default;
- we protect data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data;
- we maintain documentation required by law, including appropriate data protection policies;
- we admit to the processing of data exclusively persons with appropriate authorization;
- we keep the records of persons authorized to process personal data;
- we ensure control which personal data, when and by whom has been transferred to us and to whom it is transferred.

In particular, we use the following technical measures that prevent unauthorized persons from getting access to information and personal data processed through the Website:

- cryptographic measures in the form of a VPN tunnel and encrypted SSH connection;
- Amazon firewall systems;
- authentication with the use of RSA and DSA keys.

Specific threats related to the use of an electronically supplied service: getting unauthorized access to information concerning a User.

XI.COOKIE FILES AND SIMILAR TECHNOLOGIES

A cookie file is a small text file, which often contains an anonymous, unique identifier. Cookie files are created at the time when the User's browser loads a given website. The website sends the information to the browser, which subsequently creates a text file. Whenever the User returns to the same website, the browser downloads and sends such files to the website's server. More information about the use of cookie files is available on the website <https://wszystkoociasteczkach.pl/>.

In addition, we use other technologies (such as tracking scripts (*pixels*, *web beacons*) and in applications the so-called *software development kits* (in short usually termed as SDKs), which fulfil similar functions and which allow us to monitor and improve the Services and e-mail communication. Speaking in the Policy about cookie files, this term includes also such similar technologies. More information about our practices related to the protection of personal data and privacy, and also the purposes of the processing of personal data collected by cookie files, the User can find in the remaining chapters of this Policy.

According to the purpose of their use, cookie files used by us can be divided into the following categories:

a) Necessary cookie files

These files are necessary to ensure basic functionalities of the Services. Without them it is not possible to use the requested services, such as e.g. logging in to the PLL LOT account, filling in a booking form. In the case of disabling such cookie files, some elements of the Services may become inaccessible to the User (e.g. logging in to the PLL LOT account, filling in a booking form). These files are also necessary to ensure the safety of using the Services.

b) Analytical cookie files

These files help us improve and optimize Users' experiences related to the use of the Services. They help us measure the way of using the Services, so that we can improve their functioning and comfort of use (including to test new functionalities or correct errors). These files are used to collect technical and analytical data, such as recently visited pages in the Website, number of visited pages, information on getting acquainted with e-mail communication, information about clicks in different parts of the Services and e-mail communication, as well as on the time between different clicks.

c) Functional cookie files

We may use cookie files, which are not necessary for using the Website, however, they allow to use some functions. These files, for example, collect information concerning the User's interactions with services offered in the Services and may be used in order to remember the User's preferences (such as choice of language / currency), interests and the way of presentation of the website (such as font size). We may ask the User's permission for using such cookie files when they want to use a specific functionality in the Services.

d) Advertising cookie files

We use these files in order to collect information concerning the way of using the Services, in order to adjust advertisements to the User and their possible interests or preferences. In addition, they are used to limit the number of displays of the same advertisement and to measure the effectiveness of advertising campaigns. We may make available this information to other entities which help in the management of internet advertisements – more details are available below in the part "Third Parties".

Third Parties

The use by the User of the Services may cause using some cookie files which we do not control. This may take place in a situation when the part of the Website visited by the User uses third parties' tools for data analytics or automatization/marketing management or contains content displayed from third parties' websites such as e.g. YouTube or Facebook. We recommend getting acquainted with the privacy and cookie files policies of these services in order to find out in what way these entities use cookie files and if the User's data from cookie files are transferred to third countries. The list of third parties which place cookie files in the Services is below.

Purpose	Third party	Retention period
Analytics	Adobe	24 months

	Criteo	24 months
	Rental cars	24 months
	Booking.com	24 months
Functionality	[]	[]
Advertisements	Adobe	12 months
	Google Inc	13 months
	Bing	24 months
	Facebook	24 months
	Criteo	12 months
Social media	Facebook	[]

How long will we process your data?

We store the information collected from cookie files for [maximum period 24 months].

How can you manage cookie files?

The User may, at any time, gain access and make changes of their preferences concerning cookie files by clicking [here].

Browser settings

The User may express their decision whether they express their consent to the saving cookie files also on their device through browser settings. More information

about what options are offered by the browser, including how to change cookie files saving settings and how to delete previously saved files, the User can find in the following links concerning the most popular browsers:

1. [Microsoft Edge](#)
2. [Mozilla Firefox](#)
3. [Chrome](#)
4. [Opera](#)
5. [Safari](#)

If the User would like to avoid cookie files (*web beacons*) in e-mail communication, the User may make changes in the settings of the program for reading e-mails and disable the functionality which enables remote loading of images and refrain from clicking on links.

XII. SPECIAL RULES CONCERNING THE PROCESSING OF THE DATA OF PASSENGERS TRAVELLING BETWEEN THE EUROPEAN UNION AND THE UNITED STATES

Due to the fact that the Passengers of PLL LOT travel between the European Union and the United States, below we present special rules concerning the processing of their personal data

- PLL LOT, according to US law and the international agreement between the European Union and the United States, will transfer PNR data to the United States Department of Homeland Security (hereinafter referred to as "DHS"). This data shall be transferred for the purposes set out in Chapter IV of the Policy.
- PLL LOT will transfer the Passenger's data collected before the travel (Advance Passenger Information – API i.e. in particular information from the Passenger's passport that are collected during the check-in) to border control authorities. This data shall be transferred for the purposes set out in Chapter IV of the Policy.
- In order to obtain exhaustive explanations on the manner of handling PNR data concerning flights between the European Union and the United States by DHS, one can become acquainted with the obligations of the United States Department of Homeland Security ("PNR Obligations") published in the US Federal Register vol. 64, No. 131, page 41543.
- PNR data received in connection with flights between the EU and the USA may be made available to other domestic and foreign governmental authorities responsible for combatting terrorism or law enforcement for the purposes set out in Chapter IV of the Policy.
- Some PNR data belonging to special categories of data within the meaning of 9 GDPR can be entered in the PNR if they are transferred to DHS from community booking systems or air carriers departure control. Such PNR data, which belong to special categories of data, include in particular, certain information on the Passenger's racial or ethnic origin, their political views, religious convictions, health condition or sexual orientation. DHS has undertaken not to use any PNR data belonging to special categories of data, which they receive from booking systems or air carriers departure control in the EU. DHS has launched an automatic filtering program, preventing the use of PNR data belonging to the category of special PNR data.
- PNR data from flights between the EU and the USA will be stored by DHS for 3 years and six months, unless DHS, during this time, makes manual access to this particular PNR data. In

such cases, PNR data will be stored in DHS for an additional period of eight years. Moreover, information related to particular enforcement records will be kept in DHS by the time such a record is archived.

- The obligation to ensure that all DHS departments handle personal information in accordance with the relevant act rests with the Chief Privacy Officer in the Department of Homeland Security. This Officer is independent from all DHS directorates, and their findings are binding for the entire department. In order to ensure that DHS strictly follows provisions and uses proper safety measures, they will exercise general supervision over the program.
- Every passenger may demand from DHS additional information on the type of PNR Data made available to DHS and ask to be issued a copy of data included in DHS database. To the extent it is permitted by the Freedom of Information Act and other statutory and implementing provisions and political objectives, regardless of the Passenger's nationality or place of residence, DHS will consider the request concerning documents, including also PNR documents possessed by DHS. DHS can refuse to disclose or postpone the disclosure of all PNR data or part of them in certain circumstances (e.g. if there are reasons to expect that it will disrupt pending legal proceedings or cause a disclosure of techniques and procedures used during investigations conducted by law enforcement authorities). If DHS refuses access to PNR data under the departures set out in the Freedom of Information Act, there is a possibility to lodge an appeal from this decision by virtue of administrative procedure to the Chief Privacy Officer in DHS, who on behalf of DHS is responsible for both privacy protection and data disclosure rules. The final decision is actionable in court under the provisions of US law.
- Passengers may demand rectification of their PNR data included in DHS databases, contacting the following offices. DHS will take into account these rectification requests which they find justified and properly substantiated.
- Enquiries concerning PNR data made available to DHS or requests for making data possessed by DHS and relating to the requesting party available should be sent in writing to: Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229. Further information concerning the procedures of submitting such requests can be found in section 19 Code of Federal Regulations, section 103.5. If someone wants to report a problem or complaint concerning PNR data or submit a request for their correction, this can be done in writing to the address: Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229. Decisions of DHS are subject to verification of the Chief Privacy Officer in the Department of Homeland Security, Washington, DC 20528. Any enquiries, complaints or requests for the rectification of PNR data can be also addressed to a data protection authority in the EU member state of a given Passenger for possible further examination.
- If the complaint cannot be settled by DHS, the person submitting a complaint can address in writing the Chief Privacy Officer in the Department of Homeland Security: Chief Privacy Officer of the Department of Homeland Security, Washington, DC 20528. The Chief Privacy Officer will assess the situation and try to settle the dispute. One can also submit a complaint through the national data protection authority (hereinafter referred to as "DPA") i.e. the President of the Data Protection Office (UODO President). The Chief Privacy Officer has undertaken to handle complaints received from data protection authorities of EU member states on behalf of an EU citizen, if the citizen authorizes them to act in their case.
- More information on the manner of using personal data by airlines can be obtained directly from airlines in a given country.

Regardless of the above information, the transfer of personal data to countries from outside the European Economic area takes place in accordance with the rules set out in Chapter V of the GDPR.