Privacy Policy

Effective Date: September 5 2024

Review Date: September 5 2024
API Combined Privacy Policy Version 12 (internal 10.10)

Introduction

Lodging Solutions LLC d/b/a Accommodations Plus International ("API") respects the privacy of visitors to our website, users of our services, including services provided to passengers and crew members and other employees of our clients. We recognize the need for appropriate protections and management of personal information that may be provided by your employer to API, and personal information that you may provide to us as part of our services. This Privacy Policy will assist you to understand what types of information we may collect, how that information may be used, and with whom the information may be shared. You may also wish to review your own employer's Privacy Policy or your chosen travel carriers Privacy Policy, for more information about how your personal data is collected, used and shared. API serves as both Controller and Processor (or Service Provider). When you engage API, for Software as a Solution services, API is acting in capacity as a Processor, API is not responsible for the policies or practices of our clients, which may differ from those disclosed in this Privacy Policy. For all other services where we collect personal data, API is a Controller.

API provision of services to our clients, are not publicly available.

Data Protection Laws

California

If you are a California resident, please click **here** for additional California-specific privacy disclosures.

United Kingdom and European Union

If you are a United Kingdom or European resident, please click **here** for UK and EU specific privacy disclosures.

What categories of personal information do we collect and purpose?

Personal Information for purposes of this Privacy Policy is information that identifies or can identify a specific individual including:

1. Individual's name, employee number, crew position (e.g., captain, first officer, flight attendant, or job title, etc.), base location (domicile), hire date, gender (only for specific airlines and cruise lines), associated flight, ship, deadhead, pairing, department, and accounting information as may be provided by your employer for the purposes of performance of the individual's work-related activities.

2. Information that associates individuals with assigned hotels and ground transportation providers as part of the individual's work-related activities. This may include additional room / pick-up information such as confirmation numbers.
3. Passenger name, PNR, email address, phone number, information relating to limited mobility, provided by your chosen carrier.
4. Cell phone or e-mail address information, as may be provided by you or your company, to receive work-related e-mails and/or SMS text messages. You have the ability to opt into and out of this service as contractually agreed-to with your employer.
5. Per diem (allowance) information may be obtained, derived, used and retained expressly as contractually agreed between API and your employer.
6. Information that an individual may voluntarily provide as feedback to API for a specific hotel or ground transportation service and layover experience.
7. Audit logs of user activity on API websites, such as date/time stamps, used in accordance with industry-standard security practices.
8. My Crew Care Application stores your user profile for the persistent login feature of the application.
9. During client events, negotiation and onboarding processes, API will collect your personal data, which includes your name, email address and contact telephone number. This includes communications before using or supporting any of API's services and post contract, whilst using any of API's services.
10. Website users/visitors, personal identifiers, information collected by cookies and other technologies, including IP address, including API application log information and user profile.
11. Business Partners and Business to Business Communications and Negotiations, which may include name, email address and telephone number.
12. Verbal and/or email exchanges with you, regarding any of our Software as a Solution service or service that you can provide to API. During the course of this communication and/or negotiations, we will collect your personal data, which includes your name, email address and contact telephone number.
13. Business development, networking, completion of surveys and arranging events.

In some circumstances, API may collect personal information from you, which may be regarded as special category of personal data or sensitive information. This may include your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data health details regarding sex life / sexual orientation.

We will only collect special category of personal data, where you have given your explicit consent and where necessary, directly related to one or more of our Services as a Solution(s).

My Crew Care Application

When accessing the My Crew Care mobile application, you will be presented with a range of optional functions the application could have access to, such as location data, phone data, photos/media/ files, storage, camera and other data.

To enable your mobile device to access any of the features listed above, you will be asked for your explicit consent by a pop-up notification. It is your choice whether you enable any of these features by accepting the pop-up notification.

The My Crew Care application will only store your user profile. It does not store any other personal data, even if you enable any of the functions listed above, by accepting the pop-up notification.

How do we get your personal information and why we have it

API will either receive personal information from you, as a result of your employer or travel provider engaging API to provide Software as a Solution Service(s).

In any other instance, API will receive personal information from you or publicly available and paid sources or from conference and industry events

With whom does API share personal information?

API may collect, share, disclose or make available, as required, for the provision of our services:

1. API primarily provides personal information (such as name, employee ID, rank, and arriving/departing flight/cruise information) to third party hotel and ground transportation companies in accordance with API's contractual agreements with your employer. For selected clients, API may also provide per diem (allowance) information to hotels in accordance with the contractual obligations with your employer.
2. API primarily provides personal information of passengers to third party hotel and ground transportation companies, in accordance with API's contractual agreements with your chosen carrier.
3. API may provide personal information to third-party hotel booking engines and tools (including Global Distribution Systems) as may be necessary for fulfillment of our obligations to your employer
4. API may provide any and all personal information we have in our databases with your employer. This information may be included in reports, invoices, data marts etc.
5. General database information may be shared with our software development partners for the sole use of analysis, programming, testing, monitoring and quality assurance of our technology solutions.
6. We may provide personal information to national or law enforcement agencies as required by applicable law, or if we feel this action is necessary to protect our business, employers, suppliers or customers.
7. Your personal data is shared internally, with our team, on a need-to-know basis.
8. In the normal course of our provision of services to your employer and in accordance with our contractual obligations to your employer, we may share your personal data with approved sub processors.
9. In the normal course of our provision of services to your chosen carrier and in accordance with our contractual obligations to your chosen carrier, we may share your personal data with approved sub processors.
10. We share your personal data with third party service providers, such as Microsoft Services, AWS, Sales Force, marketing software products, facsimile software and Google Forms.
11. We share your personal data with our partners (including developers), subcontractors and agents as necessary to fulfill and support our Services as a Solution.

Unless permitted by relevant laws, or you have agreed to this, API will not share personal information or sensitive information you provide to API with any other third parties without your consent or sell, trade or lease your personal information to others, except as provided in this Privacy Policy.

Wherever possible the data shared are either anonymized and/or minimized and only those with a valid business 'need to know' in the receiving organization are granted access.

Choice and Consent

API receives and/or processes your personal information as part of a contractual services agreement with your employer or chosen travel carrier. For any optional services that API provides, such as receiving email or text messages of hotel changes or notifying you of events, you will have the ability to opt into or out of these optional services.

How do we protect your personal information?

While no online services can guarantee absolute security, we have implemented appropriate technical and organizational measures to protect the personal information that we collect and process. API is committed to continually evaluating and updating these measures in order to protect your privacy.

International data transfers

The personal information we collect may be transferred to, and processed in, countries other than the country in which you reside. These countries may have data protection laws that are different to the laws of your country (and, in some cases, may not be as protective). While such information is outside of your country of residence, it is subject to laws of such other countries, and may be subject to disclosure to the governments, courts or law enforcement or regulatory agencies of such other country, pursuant to the laws of such country.

Specifically, the servers of our Online Services are in the USA, unless agreed otherwise.

Compliance with the EU-U.S. Data Privacy Framework and the UK Extension to the EU-U.S Data Privacy Framework and the Swiss-U.S Data Privacy Framework

On July 10, 2023, the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework ("EU-U.S. DPF") entered into force, as the successor to Privacy Shield. The EU-U.S. DPF Principles entered into effect, the same date.

API complies with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. API has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. API has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF.

If there is any conflict between the terms in this Privacy Policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/s/program-overview

API, does not have any other U.S. entities or U.S. subsidiaries. API is the only organization in scope of and will adhere to the EU-U.S. DPF, the UK Extension to the EU-U.S DPF and Swiss-U.S DPF.

We have certified that we adhere to the Principles of Notice, Choice, Accountability for Onward Transfers, Security, Data Integrity and Purpose Limitation, Access, and Recourse Enforcement and Liability, in accordance with the EU-U.S DPF, the UK Extension to the EU-U.S DPF and Swiss-U.S DPF

We will only process personal information in ways that are compatible with the purposes outlined above, in this Privacy Policy and uphold the rights of EU, UK and Swiss individuals.

As explained in this Privacy Policy, we may provide your personal information to third parties who perform services on our behalf. If we transfer personal information received under the EU-US DPF, the UK Extension to the EU-U.S DPF and the Swiss-U.S DPF to a third-party agent or service provider and they process your personal information in a manner inconsistent with the EU-US DPF, the UK Extension to the EU-U.S DPF and the Swiss-U.S DPF, we will remain liable if they fail to meet those obligations and we are responsible for the event giving rise to damages, unless we can prove we are not responsible for the event giving rise to the damage. API complies with the EU-US DPF Principles, the UK Extension and the Swiss-U.S DPF Principles for all onward transfers of personal data from the EU, UK and Switzerland, including the onward transfer liability provisions.

Under certain circumstances, we may be required to disclose your personal information in response to valid requests by public authorities, including to meet national security or law enforcement requirements.

You have the right to access personal information that we hold about you, including the right to object to the processing, and the right to have data rectified and erased.

If you have any inquiries or complaints about our handling of your personal information under the EU-US DPF, the UK Extension to the EU-U.S DPF and the Swiss-U.S DPF, you should first contact us at **privacy@apiglobalsolutions.com** and we will respond to your inquiry promptly. If we are unable to satisfactorily resolve your complaint, or we fail to acknowledge your complaint in a timely fashion, we have further committed to cooperate and comply with the panel of European Data Protection Authorities (DPAs) in the resolution of any EU-US DPF, the UK Extension to the EU-U.S DPF and the Swiss-U.S DPF, complaints. Individuals may also have the opportunity under certain conditions to invoke binding arbitration for complaints regarding the EU-US DPF, the UK Extension to the EU-U.S DPF and the Swiss-U.S DPF, not resolved by the above mechanisms. See here for additional information about binding arbitration.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, API commits to resolve DPF Principles-related complaints about our collection and use of your personal data. EU and UK and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF should first contact:

Lodging Solutions LLC d/b/a Accommodations Plus International (API) at:

Accommodations Plus International
Attn: Senior Information Risk Officer
265 Broadhollow Road
Melville, NY 11747

For non-human resources personal data, API has committed to refer unresolved EU-US DPF and the UK Extension to the EU-US DPF and the Swiss-US DPF complaints to JAMS, an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your DPF Principles related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://www.jamsadr.com/DPF-Dispute-

Resolution for more information or to file a complaint. The services of JAMS are provided at no cost to you.

For human resources personal data, in compliance with the EU-US DPF, the UK Extension to the EU-US DPF, API commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPA's) and the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-US DPF and the UK Extension to the EU-US DPF, in the context of the employment relationship, for UK and EU individuals.

In the course of your employment (including contractors and the recruitment process) with API, please refer to the relevant internal company polices to understand how API processes your personal information.

The Federal Trade Commission has jurisdiction over API's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

Other International Transfer Mechanisms Transfers of Personal Data

Depending on the circumstances of the personal data processing activity, we may use an alternative personal data transfer mechanism, such as standard contractual clauses. Regardless of where we process your personal data, we protect it in the manner described in this Privacy Policy and in accordance with applicable law.

Cookies

Our Website uses cookies. Cookies are text files containing small amounts of information which are downloaded to your personal computer, mobile or other device when you visit a website. It allows the website to recognize that user's device and store some information about the user's preferences or past actions.

Cookies do not identify you personally, just the computer or device you are using. Cookies help make it easier for you to log on to and use our site during future visits, navigate between pages efficiently, remember your preferences and improve the user experience. They also allow us to monitor traffic on our site. You have the choice to opt out of cookies being placed on your device.

The cookies we use may fall into one or more of the following categories:

a) Analytics/performance cookies: Every visit generates an 'anonymous analytics cookie' which tell us whether you've visited our site before, which allows us to track how many users we have, and how often they visit our site. We use these cookies to gather statistics and maintain our site performance.

b) Functionality cookies: These allow us to remember choices you make and provide enhanced, more personal features. For example, remembering your email address and preferences on our website, so you don't have to choose them each time you visit.

c) Strictly Necessary: These are cookies that are needed for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website.

Data Protection Laws

Californian Resident Privacy Notice

This section of the document is specifically for California Residents and supplements the information contained in the API Privacy Policy, detailed in the first part of this document and can be found at https://www.apiglobalsolutions.com/. This applies solely to all visitors, users, and others who reside in the State of California ("consumers" or "you"). API provides the following notice in compliance with the California Consumer Privacy Act of 2018 (CCPA) and other California laws and regulations, applies solely to California Residents. It also describes your choices and rights under the CCPA.

Personal Information we Collect

The personal information that API may collect and that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device, is set out in this Notice.

For the purposes of this Notice, personal information does not include:

- Publicly available information from government records;
- Deidentified or aggregated consumer information;
- Information excluded from the CCPA's scope.

The API Privacy Policy sets out the categories of personal information.

Purposes for Collecting Personal Information

API's Privacy Policy sets out how we use your collected personal information. API will not collect additional categories of personal information or use the personal information we collected for incompatible or materially different purposes, without providing you notice.

API does not sell or share personal information of consumers under 16 years of age.

Sharing your Personal Information

Who we share your collected personal information with, is detailed in API's Privacy Policy.

Disclosures of Personal Information for a Business Purpose

In the preceding twelve (12) months, API has disclosed the categories of personal information for a business purpose, as set out in API's Privacy Policy.

Sales of Personal Information

In the preceding twelve (12) months, API has not sold your personal information.

Your Rights and Choices

The CCPA provides California residents (consumers) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise these rights.

Right to Know and Access Personal Information

You have the right to request that API disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

1. The categories of personal information we collected about you, in the preceding 12 months
2. The categories of sources for the personal information we collected about you
3. Our business or commercial purpose for collecting, selling or sharing your personal information
4. The categories of third parties to whom we disclose your personal information;
5. The specific pieces of personal information we collected about you.

Right to Delete Personal Information

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions.

Once we receive, confirm and verify your request, we will delete (and direct our service providers and contractors to delete) your personal information from our records and notify all third parties to whom the business has sold or shared such personal information, to delete the consumer's personal information, unless this proves impossible or involves disproportionate effort.

We may refuse your deletion request and retain your personal information in the following circumstances:

1. Complete the transaction for which the personal information was collected, fulfil the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
2. Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes.
3. Debug to identify and repair errors that impair existing intended functionality.
4. Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
6. Engage in public or peer reviewed scientific, historical, or statistical research that *conforms or* adheres to all other applicable ethics and privacy laws, when the business's deletion of the information is likely to render impossible or seriously impair the *ability to complete* such research, if the consumer has provided informed consent.
7. To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business *and compatible with the context in which the consumer provided the information.*
8. Comply with a legal obligation.

Right to Correct Inaccurate Personal Information

You have the right to request that your personal information that we collected from you, is accurate.

Once we receive, confirm and verify your request, we will correct your inaccurate personal information.

Right to Know what Personal Information is Sold or Shared with Whom

You have the right to request information from API, if your personal information is sold or shared for a business purpose.

API does not sell your personal information.

The API Privacy Policy details who we share your personal information with, which does not include sharing your personal information for advertising purposes.

Right to Opt Out of Sale or Sharing Your Personal Information

You have the right to opt out of the sale of your personal information. API does not sell your personal information.

You have the right to opt out of sharing your personal information for advertising purposes. API does not sell your personal information for advertising purposes.

Right to Limit (Restrict) Use and Disclosure of Your Sensitive Personal Information

You have the right, at any time, to direct API that collects sensitive personal information about you, to limit its use of your sensitive personal information to that use which is necessary to perform the services or provide the goods. API does not collect your sensitive personal information.

Methods to Limit Use of Sensitive Personal Information

You have the right to limit our use of your sensitive personal information. API does not collect any of your sensitive personal information.

Right to be free from Discrimination

We will not discriminate against you for exercising any of the rights described above. Unless otherwise permitted by law, we will not deny you goods or services, provide you with a different level or quality of goods or services, or charge you different prices or rates for goods or services because you have exercised your rights described in this Notice.

Exercising your Rights

To exercise your rights described above, please submit a verifiable consumer request to us by either:

Calling us at: 1-516 798 4444 (please ensure that you advise our team, that your call relates to privacy).

Emailing: privacy@apiglobalsolutions.com or writing to us at:

Lodging Solutions LLC d/b/a Accommodations Plus International (API) at:

Accommodations Plus International
Attn: Senior Information Risk Officer
265 Broadhollow Road
Melville,
NY 11747

Or by completing Californian Notice Request Form **here**.

Only you, or someone legally authorized to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child (if applicable).

You may only make a verifiable consumer request for your right to know/right to access and right to know what personal information is shared or sold with whom, twice within a 12-month period.

The verifiable consumer request must:

(1) provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative; and

(2) describe your request with sufficient detail that allows us to properly understand, evaluate and respond to it. We will verify your identity by asking for certain identifying information and matching that against the information we have on file. In certain cases, we may need to ask for more information.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

Making a verifiable consumer request does not require you to create an account with us.

Response Timeline

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time, we will inform you of the reason and extension period in writing.

We will deliver our written response by using your account, mail or electronically or in a readily useable format that allows you to transfer your information from one entity to another, at your option.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

California Do Not Track Disclosures

Privacy regulations in California require API to indicate whether it honors your browser's "Do Not Track" settings concerning targeted advertising. API does not monitor or respond to Do Not Track browser requests.

Privacy Notice for United Kingdom and European Union Residents

This section of the document is specifically for EU and UK residents.

Lodging Solutions LLC d/b/a Accommodations Plus International ("API") is the Controller under the UK General Data Protection Regulation and EU General Data Protection Regulation ("GDPR"), including national implementing legislation, for the purposes listed above.

You may contact API to make requests, for example to exercise your data protection rights, to provide positive feedback or to make complaints by writing to us at the address below.

Our Contact Details in the USA and Representative in the UK and EU

Name: Lodging Solutions LLC d/b/a Accommodations Plus International (API)
Address: API Inc, 265 Broadhollow Road, Melville, NY 11747, USA

Phone Number: 1-516 798 4444 (please ensure that you advise our team, that your call relates to privacy).

Data Protection Officer Email: privacy@apiglobalsolutions.com

EU GDPR Representative

API have appointed Fifth Square Limited as its Representative under the EU GDPR. This Representative may be contacted at:

Name: Rune Pettersen

Address: Coolharbour, Roundwood Co. Wicklow A98 FY68, Ireland

Email: eurep@fifthsquare.eu

The Representative has been appointed as the criteria set out in Article 3(2), EU GDPR are met, specifically:

"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union"

UK GDPR Representative

API have appointed Fifth Square Limited as its Representative under the UK GDPR. This Representative may be contacted at:

Name: Simon Ghent

Address: 36 Pine Walk, Weybourne, Holt, Norfolk, NR25 7HJ, United Kingdom

Email: simon@fifthsquare.co.uk

The Representative has been appointed as the criteria set out in Article 3(2), UK GDPR are met, specifically:

"This Regulation applies to the processing of personal data of data subjects who are in the United Kingdom by a controller or processor not established in the United Kingdom, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the United Kingdom"

What is the lawful basis to process your personal information

API collect and use this information under provisions contained in the GDPR. Specifically, we collect the information referred to above in the 'purposes' section, under the requirements of legitimate interests of networking, to grow the business and to develop our partnership with our suppliers and partners and to improve our site and performing certain services.

Details of transfers of personal information to any third countries and safeguards

API is located in the USA.

Depending on the purpose and the type of personal information processed, your consent allows us to transfer your personal data to the USA and contact you for the purposes outlined above

You can withdraw your consent at any time, by using the contact details provided in this Privacy Notice.

We share your personal data with the entities detailed above and we may transfer your information to jurisdictions/countries that may not provide the same level of data protection as your home country. To protect such information, transfers will be made as permitted by applicable law, including where necessary being subject to appropriate standard contractual clauses. Regardless of where we process your information, we protect it in the manner described in this Privacy Notice and in accordance with applicable law.

Retention period or criteria used to determine the retention period

Your personal data will be kept in accordance with our Retention Policy.

How we store your personal information

Your information is securely stored.

We keep all your personal data, detailed in this Privacy Notice, for business development purposes and ongoing business to business relationship, for a period specified in our Retention Policy.

Your data protection rights

You have the right to exercise the following rights under the GDPR. These rights are not absolute and will depend on which legal basis we use to process your personal data.

Please contact us using the contact details set out above if you wish to exercise any of these rights:

- **Transparency** – we must provide you with all the information set out in this Privacy Notice in a concise, transparent, intelligible and easily accessible form, using clear and plain language, so that you may understand how and why we process your data and what your rights are. We must keep you informed in timely manner about our progress in responding to requests from you to access your rights under data protection law.

- **Rights of access by the data subject** – you have the right to obtain from us confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, to access your personal data.

- **Right to rectification** – you have the right to have the personal data concerning yourself rectified without undue delay, if it not accurate. Taking into account the purposes of the processing, you also have the right to have incomplete personal data completed, including by providing a supplementary statement.

- **Right to erasure ('right to be forgotten')** – in some limited circumstances, you may have the right to obtain from us the erasure of your personal data without undue delay, when and if:
    - Processing your personal data is no longer necessary in relation to the purposes for which your data were collected
    - Where you withdraw consent for processing, but only if consent was the legal basis relied upon for that processing
    - You object to processing and there are no overriding legitimate grounds for the processing or where you withdraw your consent to marketing. NB This does not apply to employees or former employees or applicants where we have a legal obligation to retain your data
    - Your personal data has been unlawfully processed
    - Your personal data has to be erased to comply with a legal obligation to which the Controller is subject
    - Your personal data has been collected in relation to the offer of information society services to children

- **Right to restriction of processing** – In some limited circumstances you have the right to request that the processing of your personal data is restricted, in some cases for a limited time only, specifically when:
    - You are contesting the accuracy of your personal data while we verify its accuracy or correct it
    - The processing is unlawful and you oppose the erasure of your data;
    - Where we no longer need your personal data for the purposes for which it was obtained but where you require the data for the establishment, exercise or defence of legal claims
    - Where you have objected to the processing of your data pending the verification whether legitimate grounds of the Controller override your interests.

  - You have the right to be informed by the Controller before the restriction of processing is lifted

- **Notification obligation regarding rectification or erasure of personal data or restriction of processing – we will let you know when the following things happen, unless is proves impossible or disproportionate to do so:**
  - When we have rectified your data
  - When we have erased your personal data
  - When we have restricted the processing of your personal data
  - When we intend to lift any restriction to the processing of your personal data
  - We will also advise you about any recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort

- **Right to data portability** – upon your request and where the legal basis for processing your personal data is 'consent' or 'contract', we will provide you with a copy of your personal data that you have provided to us and which are processed by automated means, in a structured, commonly used and machine-readable format. Upon your request and where technically feasible, we will also transmit those data to another data controller.

- **Right to object** – In some limited circumstances, you have the right to object to our processing of your personal data. When certain conditions are met we, as Controller, will no longer process your personal data. This right can be exercised only when:
  - Either the processing is necessary for the performance of a task carried out in the public interest or processing is necessary for the purposes of our legitimate interests (including profiling), but where we cannot demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or where processing is necessary for the establishments, exercise or defence of legal claims
  - Processing for direct marketing purposes, including profiling
  - When personal data are processed for scientific or historical research purposes or statistic purposes unless the processing is necessary for the performance of a task carried out for reasons of public interest

- **Automated decision-making, including profiling** – you have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significant effects. At the current time API does not perform automated decision making or profiling.

- **Details of whether you are under a statutory or contractual obligation to provide the personal data –** this is not applicable to API.

- **The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences –** API does not currently perform automated decision making or profiling.

How to complain

If you have any concerns about our use of your personal data, you can make a complaint to us, by using the contact details provided above, in this Privacy Policy.

You can also complain to the UK ICO if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk

You can also complain to the Data Protection Commission in Ireland:

21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland

Helpline number: 01 7650100 / 1800437 737

Data Protection Commission website: https://www.dataprotection.ie/

Changes to This Privacy Policy and How to Contact Us

Updates to this Privacy Policy

Changes to this Privacy Policy will be made when required in response to changing legal, technical or business developments. When we update our Privacy Policy, we will take appropriate measures to inform you, consistent with the significance of the changes we make, and in accordance with applicable law. You can see when this Privacy Policy was last updated by checking the "Effective Date" and last reviewed by checking the "Review Date" displayed at the top of this Privacy Notice.

If you have any questions about changes to this Privacy Policy, please contact us at the information below.

How to contact us

If you have any questions or concerns about our use of your personal information and information within this Privacy Policy, please contact us via the Contact Us Section on our customer services portal **here**.

If you have any further questions or are unsatisfied with our response to any data protection issues you raise with us, you have the right to contact the appropriate Data Protection Authority within your Country or Region which is tasked with the protection of personal data and privacy.