Arbitration Ireland

PRIVACY POLICY 2019

As a visitor to our website, Arbitration Ireland respects your right to privacy. This policy outlines our commitment to you in this regard. All instances of 'us' or 'we' or 'our' etc., in this policy refers to Arbitration Ireland. We do not actively collect personal data from visitors, but personal information volunteered to us (e.g., via the contact page of our website) will be treated with the highest standards of confidentiality.

RELEVANT LEGISLATION

Along with our business and internal computer systems,this website is designed to comply with the following legislation with regard to data protection and user privacy: EU Data Protection Directive 1995 (DPD) and EU General Data Protection Regulation 2018 (GDPR)

IDENTITY

Arbitration Ireland is headquartered at Church Street, Dublin 7, Ireland. Enquiries regarding data collected by us may be referred to Executive Director, Rose Fisher, at rfisher@arbitrationireland.com. We are the Data Controllers for any data collected by our company.

WEBSITE

We do not directly collect personal data on clients of our company or visitors to our website unless it is presented by the clients or visitors themselves (e.g., contacting us by email through the website). We do not store visitor information on this website's own database. Emails via the website are not stored on the website, but are processed through standard email protocols (as if you are using your own email system to contact us). Internet sites (including Arbitration Ireland) use some cookies (small text files) to operate properly, for example to allow visitors to negotiate between pages. This data does not identify persons to us and we do not collect such data. These cookies are set to expire when the browser session ends (is closed down). These are often referred to as session (first-party) cookies. Google Analytics, which utilises third-party cookies, is active on our website. These track use of the website but none of this information personally identifies you to us. We do not have access to all data collected via Google Analytics. Google Analytics does process some data (identifying what people look at on our website) on our behalf, and complies with relevant EU legislation, even if some data may be held outside of the EU. Please see Google (Privacy Policy) for further information.

ABOUT THIS WEBSITE'S SERVER

This website is hosted by Register365.com (Namesco Ireland Limited; Register365.com is part of the Dada Group). Full details about Register365 can be found here. All traffic (transferral of files) between this website and your browser is encrypted and delivered over HTTPS.

DATA RETENTION

We do not retain data on visitors unless they contact us directly. In the event of a contact by email via the website, this email is deleted after 12 months if there is no further contact. However, any such emails that have created a response giving an opinion or other element of service, may be retained separately.

DATA BREACHES

We will report any unlawful data breach of this website's database or the database(s) of any of our third-party data processors to any and allrelevant persons and authorities within 72 hours ofthe breach if itis apparentthat personal data stored in an identifiable manner has been stolen.

CHANGES TO PRIVACY POLICY

This policy may change from time to time in line with legislative or regulatory developments. We recommend that you check this page occasionally for any policy changes.

CONSENT STATEMENT RE EVENTS

Statement

The data that is collected will be used by Arbitration Ireland to plan and manage the event for which you registered, as well as email you relevant details about the event.

EVENT TERMS & CONDITIONS

Summary

Payment for all events will need to be paid in full prior to attending.

Full Terms & Conditions

Cancellation Policy: Under the Arbitration Ireland cancellation policy, you have the right to cancel your booking at an event under these following terms:

- If you cancel your attendance at least 14 days before the date of the event is due to begin, you will be due a full refund of that amount.
- If you cancel your booking at an event less than 14 working days before an event is due to begin, or if you fail to attend an event ,no refund will be given. Bookings are transferrable if Arbitration Ireland is given 2 working days' notice of the transfer – it is not always possible to guarantee that seating plans and other marketing material will have the revised member/company name.
- Bookings made between 3 and 14 days of the event can be cancelled within 48 hours of purchase for a full refund.
- Bookings made within 3 days are all final.

To request a cancellation or to make a change please send an email to info@arbitrationireland.com

EVENT PRIVACY POLICY

Summary

We will collect the information we need to provide you with the products and services you have requested from us. We will collect information we need to arrange events and the administration of events. This is likely to include dietary requirements and any other pertinent information related to your requirements.

FULL PRIVACY POLICY

This privacy statement sets out our policy in relation to the holding and using of information, including information which we may obtain from you when you contact us via the website or via our Tito-run event booking system. We will only use your personal information in accordance with the Arbitration Ireland Data Protection Policy. We do not actively collect personal data from visitors, but personal information volunteered to us (e.g., via the contact page of our website) will be treated with the highest standards of confidentiality.

As an Arbitration Ireland member you consent to allow Arbitration Ireland to use the information you provide for the purpose of administering your membership.

It is intended that by providing personal information about yourself to us you consent to its use for the purposes stated in the relevant data protection statement. If at any time you would like us to stop using your details for any of the above purposes, please email info@arbitrationireland.com

This privacy statement does not cover the links within this site linking to third-party websites except for Tito.io (associated with our events). You should read the privacy statements on the third-party websites you visit.

We keep our privacy statement under review and it may change. Please check our privacy statement from time to time prior to your use of the website.

EVENT DATA RETENTION POLICY

Duration: 12 months

Description: We will retain your data for 12 months post event.

Arbitration Ireland Data Protection Policy

ARBITRATION IRELAND: Adopted 12 January 2021

1. POLICY OVERVIEW

1.1 POLICY STATEMENT

1.1.1 Everyone has rights with regard to how their personal information is handled. During the course of our activities at Arbitration Ireland we will collect, store and process personal information and we recognise the need to treat it in an appropriate and lawful manner and in accordance with this Data Protection Policy (the "DP Policy").

1.1.2 The types of information that we may be required to handle include details of current, past and prospective members, employees, suppliers, and users of our services, partners, consultants and others with whom we communicate. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in European data protection laws. These laws impose restrictions on how we may use that information.

1.1.3 This DP Policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this DP Policy will be taken seriously and may result in disciplinary action.

1.2 DEFINITIONS

Term	Definition
Data Controller	is any person or organisation that determines the purposes for which, and the manner in which, any Personal Data is Processed. Arbitration Ireland is a Data Controller of member data.
Data Processor	is any person or organisation that Processes Personal Data on behalf of and under the instructions of a Data Controller.
Data Subject	means all living individuals about whom Arbitration Ireland holds Personal Data. A Data Subject need not be an Irish national or resident. All Data Subjects have legal rights in relation to their Personal Data.
DP Laws	means those laws which are focused primarily on data protection including: • GDPR and Data Protection Act 2018 • Data Protection Directive 95-46-EC • Data Protection Act 1988 to 2018 • E-Privacy Directive 2002/58 • The General Data Protection Regulation
GDPR	means the General Data Protection Regulation which came into force on the 25th May 2018.
Personal Data	means data, in automated or manual form, relating to a Data Subject who can be identified from that data (or from that data and other information in the possession of Arbitration Ireland. Personal Data can be factual or it can be an opinion about that person, their actions and behaviour.
Processing/Processed/ Process	means any activity that involves use of the Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.
Sensitive Personal Data	means Personal Data that is afforded additional protection under the DP Laws because of its sensitive nature. The express permission of the Data Subject is required before Sensitive Personal Data is Processed. **Example of Sensitive Personal Data:** Racial/Ethnic Origin/ Political Opinions/ Religious Beliefs/Sex Life/ Trade Union Membership/ Physical/Mental Health/ Criminal History.

2. SCOPE

The scope of this policy extends to all Personal Data maintained by Arbitration Ireland and the processes, systems and networks that support it.

While this DP Policy applies to all individual pieces of Personal Data processed by Arbitration Ireland particular attention should be paid when Processing Personal Data that involves the following (whether in electronic or paper form):

- Databases or files includes a number of Personal Data records
- Documents or files including Sensitive Personal Data
- Personal Data of Arbitration Ireland members
- Employee and member records
- Use of devices, mobile phones/laptops that store Personal Data particularly mobile devices used externally.

2.1 DATA PROTECTION OFFICER

Arbitration Ireland Data Protection Officer ("DPO") is responsible for ensuring compliance with DP Laws and with this DP Policy. Arbitration Ireland DPO contact details are as follows:

Arbitration Ireland DPO: Rose Fisher

Email: rfisher@arbitrationireland.com

2.2 REVIEW AND APPROVAL

2.2.1 Arbitration Ireland DP Policy will be reviewed annually and approved by the Executive Committee of Arbitration Ireland

2.2.2 Any questions about the operation of this DP Policy or any concerns that the DP Policy has not been followed should be referred to Arbitration Ireland DPO as soon as possible.

2.3 DATA CLASSIFICATION

2.3.1 Information can be defined as data that has value. Arbitration Ireland will maintain a comprehensive and up-to-date listing of its information assets for the purposes of classifying the information in accordance with its value, criticality, sensitivity and legal implications. This will ensure that data is not lost, destroyed or otherwise mistreated by staff members. This list is contained in the records management policy.

2.4 DATA PROTECTION AWARENESS

2.4.1 All permanent and new staff will be provided with Data Protection awareness training to enhance awareness and to educate them regarding the range of threats to Personal Data and the appropriate safeguards and to explain their individual responsibilities.

2.5 DATA PROTECTION TRAINING

2.5.1 All new Arbitration Ireland staff will receive assessed Data Protection training.

2.5.2 Data Protection training/refresher training for all Arbitration Ireland staff must be completed every 2 years. This may take the form of completing Arbitration Ireland GDPR training, in conjunction with any informal internal staff training / awareness conducted during staff meetings / briefings. Where there are significant changes to the DP policy this requirement may be brought forward.

2.6 POLICY COMPLIANCE

2.6.1 Monitoring compliance with this DP Policy is the responsibility of the DPO in the first instance. However, it is the responsibility of all staff to report any non-compliance with this DP Policy to the DPO.

2.6.2 Any breaches of this DP Policy will be investigated and if substantiated, appropriate disciplinary action, up to and including dismissal, may be taken in accordance with Arbitration Ireland Disciplinary Policy.

3. THE DATA PROTECTION PRINCIPLES

- **PRINCIPLE 1: Lawfulness, fairness and transparency of processing**
- **PRINCIPLE 2: Purpose Limitation**
- **PRINCIPLE 3: Data minimisation**
- **PRINCIPLE 4: Accuracy**
- **PRINCIPLE 5: Storage Limitation**
- **PRINCIPLE 6: Integrity and Confidentiality**

PRINCIPLE 1: LAWFULNESS, FAIRNESS AND TRANSPARENCY	**PRINCIPLE 1 – Arbitration Ireland DP POLICY REQUIREMENTS:**
	Arbitration Ireland will ensure that: • it processes personal data received from users in accordance with the regulatory requirements of the services provided specifically: GDPR and Data Protection Act 2018 • it processes personal data in a fair and transparent manner so that the Data Subject knows what is happening with their Personal Data • where personal data is processed for the purposes of direct marketing explicit consent of the member will be sought.
PRINCIPLE 2: PURPOSE LIMITATION	Arbitration Ireland should ensure that: • it is not processing personal data in any way other than required to provide the range of Arbitration Ireland services to its members
PRINCIPLE 3: DATA MINIMISATION	**PRINCIPLE 3 –** Arbitration Ireland **DP POLICY REQUIREMENTS:**
	Arbitration Ireland will only collect the Personal Data that it needs to fulfil the purpose. Personal Data will not be Processed if it is not needed.
PRINCIPLE 4: ACCURACY	**PRINCIPLE 4 –** Arbitration Ireland **DP POLICY REQUIREMENTS:**
	Arbitration Ireland will ensure that all Personal Data is accurate and complete. Processes are in place to keep member records up to date and to correct any out of date information.
PRINCIPLE 5: STORAGE LIMITATION	**PRINCIPLE 5 –** Arbitration Ireland **DP POLICY REQUIREMENTS:**
	Personal Data will only be kept for as long as is necessary to fulfil the purpose. A data retention policy is included in Appendix 2 – Arbitration Ireland Data Retention Policy. There are processes in place to implement the retention policy and regular checks are carried out on records to ensure the policy is followed consistently.
PRINCIPLE 6: INTEGRITY AND CONFIDENTIALITY	**PRINCIPLE 6 –** Arbitration Ireland **DP POLICY REQUIREMENTS**:
	Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of the Personal Data and against its accidental loss or destruction. Arbitration Ireland IT and

	Communications Systems Policy should be adhered to at all times in additional to the requirements below: • Staff are expected to know Arbitration Ireland policies and comply with them to the extent applicable • Access to Arbitration Ireland systems will be role-based and users will be provided with the minimum access required to perform their duties • Personal Data should not be left on desks or on printers • All Arbitration Ireland systems require a unique log in and password. Passwords should have strong characteristics (e.g. 8-10 characters, alphanumeric, with special characters), passwords should not be disclosed. • Staff should lock PC/mobile devices when unattended • It is the policy of Arbitration Ireland not to disclose any personal data (e.g. account balances) over the phone or via email. • Personal Data should be securely shredded when no longer needed • Personal Data should only be saved to the designated network drives, no Personal Data or other Arbitration Ireland information should be stored on personal pc's • Laptops provided for offsite use are encrypted. • Personal Data, i.e. lists of members should not be emailed to external email accounts unless encrypted • The DPO should be notified in the event of any suspected breaches including theft or loss of equipment.

4. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

Arbitration Ireland has a policy of not transferring data outside the EEA.

None of Arbitration Ireland data processors are authorised to transfer any of the data processed outside the EEA. It is policy to include this restriction in processor contracts.

No Personal Data should be transferred to a third party outside the EEA without prior discussion and authorisation from the DPO.

5. DISCLOSURE AND SHARING OF PERSONAL DATA

In addition to the transfers referred to in Attachment 1, Arbitration Ireland may disclose any Personal Data held to third parties if Arbitration Ireland is under a duty to disclose or share Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subjects or other agreements; or to protect Arbitration Ireland rights, property, or safety of Arbitration Ireland employees, members, or others.

This includes exchanging information with other companies and organisations for the purposes of fraud protection and risk reduction.

Further information on the legitimate transfers undertaken by Arbitration Ireland is set out in Attachment 1. Arbitration Ireland DPO should be contacted for approval of any transfer falling outside those described in Attachment 1.

6. EXECUTIVE COMMITTEE COMMUNICATIONS

It is the policy of Arbitration Ireland to ensure no identifiable information is included in material distributed to Executive Committee members. Executive Committee members are encouraged to access materials online only.

7. SUBJECT ACCESS REQUESTS

Arbitration Ireland complies with the rights of members to access any personal data that Arbitration Ireland holds.

This is detailed within our Subject Access Request Handling Policy.

8 DATA PROCESSORS

8.1 SELECTION

It is the policy of Arbitration Ireland to carry out due diligence on all new data processors prior to transfer of personal data belonging to members and/or staff.

Due diligence will include the following:
1. Review of Data Processors data protection policy and other relevant policies.
2. Review of security measures that the data processor has in place to ensure security of the data while in the possession of the data processor.
3. Review of measures the data processor has in place to ensure security of the data in transit to and from the processor.
4. Review the data retention timeframes to ensure data is not retained after processing has completed.
5. Review measures that data processor has in place to ensure the safe destruction of the data.

8.2 CONTRACTS

It is the policy of Arbitration Ireland to have a contract in place with all data processors who carry out processing on behalf of Arbitration Ireland.

All Data Processor contracts will stipulate the following:
1. Processing is carried out under instruction from Arbitration Ireland
2. Data Processor is required to comply with their obligations under data protection legislation including taking appropriate steps against the accidental destruction, damage or loss of data, appropriate technical and organisational measures when processing data to secure that data against accidental or malicious disclosure or breach and ensuring its employees are appropriately trained to be compliant with data protection legislation.
3. Transfer of data to a sub-processor, 3rd party or outside the EEA requires written permission from Arbitration Ireland
4. Data Processor shall not retain data any longer than necessary for the purposes of processing and all personal data held by the data processor shall be returned to Arbitration Ireland and then deleted entirely from the data processor's systems and files on contract termination.
5. Data Processor shall notify Arbitration Ireland immediately in the event that it becomes aware of a threatened, suspected or actual breach of Arbitration Ireland Member data, if it receives a request from a Data Subject to have access to that person's Personal Data, if it receives a complaint or request relating to
Arbitration Ireland's obligations under the Data Protection Legislation or if it receives any other communication relating directly or indirectly to the processing of any Arbitration Ireland member information.

8.3 ONGOING MONITORING

It is the policy of Arbitration Ireland to reserve the right to carry out audits of its data processors. Audits will be carried out should any causes for concern arise during the course of processing.

9 BREACHES

9.1 RESPONSIBILITY OF STAFF

The Data Protection Commissioner has a wide range of enforcement powers to ensure compliance with the DP Laws. This includes the serving of legal notices compelling companies to provide information in order to assist with inquiries or compelling them to comply with a provision of the DP Laws.

The Data Protection Commissioner also has the power to investigate complaints made by a member of the public and can authorise officers to enter any property to inspect the type of information held, how it is Processed and examine the security measures currently in place.

All of Arbitration Ireland staff are obliged to cooperate fully with the Data Protection Commissioner and its authorised officers when discharging their duties.
A company, including individual members of staff, may be found guilty of failing to comply with the DP Laws or failing to comply with an information or enforcement notice issued by the Data Protection Commissioner. This could cause significant reputational damage to Arbitration Ireland.
Under the DP Laws, it is also possible that Arbitration Ireland, or any individual member of staff, could be liable for damages if Arbitration Ireland fail to observe the duty of care provision in the DP Laws or fail to comply with this DP Policy.

Arbitration Ireland will take any claims relating to a breach of this DP Policy and the DP Law very seriously and staff may be subject to disciplinary action up to and including dismissal for any breaches.

9.2 BREACH RESPONSE

Arbitration Ireland will develop a separate breach response plan. The breach response plan will address the following considerations in the event of a data breach:

1. The cause of the breach will be established as quickly as possible.
2. Immediate efforts will be made to contain the breach. If necessary, security and operations experts may be called in to assist.
3. The extent of the data breached will be established

a. the number of data subjects affected
b. the contents of the data that was breached
c. the likely duration of the data breach

4. The potential consequences for the affected data subjects will be assessed.
5. The breach will be reported to the Data Protection Commissioner within 72 hours.
6. A decision about whether to notify the potentially affected data subjects will be made based on the assessment of the consequences of the breach for data subjects.
7. The decision about whether to notify the potentially affected data subjects will be made within 72 hours of discovering the data breach.
8. The decision about how to notify the data subjects will be based on the extent of the data breach - the number of data subjects affected, the contents of the data that was breached and the likely duration of the data breach.