

Privacy Policy

Version 1.1. PDF (latest version)

Last Updated: September 2026

1. PURPOSE

- 1.1. Impress Dispute Resolutions Ltd ("IDR", "we", "us", "our") is responsible for the information we collect, use, share and otherwise process which identifies individuals ("personal information"), including users of online platforms who wish to raise disputes in relation to content moderation decisions to IDR, individuals who are referred to in the context of such disputes, visitors to our website ("Website"), and business partners (including suppliers/service providers) (collectively, "you", "your").
- 1.2. We take our responsibilities seriously including how we handle your personal information, keep it secure and comply with applicable data protection and privacy laws, including the [General Data Protection Regulation](#) (GDPR) and the [Digital Services Act](#) (DSA).

2. HOW THIS POLICY WORKS

- 2.1. The purpose of this privacy policy ("Policy") is to clearly explain when, why and how we collect and use personal information about you and the legal rights that you have in relation to this.

3. UPDATES TO THIS POLICY

- 3.1. We may amend this Policy from time to time to keep it up to date with the way we operate and to comply with any applicable legal requirements. Any updates we make will be placed on this webpage. Please regularly check these pages for the latest version of this Policy.

4. THIRD PARTY WEBSITES

- 4.1. This Policy does not apply to your use of any third-party website which we may link to on our Website.

5. DATA CONTROLLER

- 5.1. Impress Dispute Resolutions Ltd (company number 757060, registered office at 6th Floor, South Bank House, Barrow Street, Dublin 4, Ireland) is the data controller for the personal information we process in accordance with this Policy.
- 5.2. You can contact us about this Policy, or to exercise any of the rights set out below, at info@impressdisputeresolutions.org or by writing to us at the address above.

6. WHAT WE COLLECT AND OUR LEGAL BASIS

- 6.1. This Policy applies to the collection and processing of your personal information by us when you:
 - a) Submit a dispute for review by Impress Dispute Resolutions Ltd in relation to a content moderation decision concerning alleged illegal content on a content-sharing or social media platform;
 - b) Are referred to in a dispute submitted by someone else;
 - c) Use our Website;
 - d) Are in contact with us for general enquiries, events organized by us, or in relation to a complaint;
 - e) Seek to conduct business with us as a supplier, partner, or regulated entity;
 - f) Engage with us as a stakeholder, regulator (including Coimisiún na Meán), or public interest body.
- 6.2. We collect personal information during your use of our Website via cookies. For further details about our use of cookies, please refer to our [Cookie Policy](#).

7. INFORMATION OBTAINED DIRECTLY FROM YOU

- 7.1. Our process is designed to collect only the minimum amount of personal data needed in order for us to handle your dispute under Article 21 of the [DSA](#). This will typically be limited to:
 - a) Your case reference number that you have been given from the relevant online platform;
 - b) Your email address for any dispute related communications;
 - c) Your IP address to confirm your country of residence and verify jurisdiction;
 - d) Information and supporting evidence you provide to us as part of your case concerning illegal content.



- 7.2. We urge you to avoid sharing with us any unnecessary personal information about you or others as part of your case.

8. INFORMATION OBTAINED FROM ONLINE PLATFORMS

- 8.1. Online platforms will share with us their case file which is connected to your case reference number and may also include personal information about you and / or other individuals referred to in the case. The type of personal information we receive will depend on the nature of the illegal content dispute but will typically include a copy of the disputed content, supporting metadata, the platform's Statement of Reasons (as required under Article 17 of the [DSA](#)), and enforcement timestamps.

9. COMPARATIVE SCOPE OF PROCESSING VS. OTHER ODS BODIES

- 9.1. Unlike other certified Out-of-Court Dispute Settlement (ODS) bodies that may process personal data to evaluate platform-specific terms and conditions across broad categories, IDR specifically processes dispute data to evaluate allegations of illegal content under applicable Irish and EU laws. Our data processing is strictly limited to communications conducted in English.

10. CATEGORIES OF DATA, PURPOSES, AND LAWFUL BASES

- 10.1. The table below sets out the categories of personal information we collect, why we use each, and the lawful basis we rely on for processing it.

Types of Personal Information	Purpose	Legal Basis
User ID Data: Case reference number, email address, IP address	To allow us to verify your identity, confirm jurisdiction, and mitigate against abuse of process or fraudulent submissions.	Legitimate Interest: To verify user identity, protect operational integrity, and prevent fraudulent claims.
Dispute Data: Email address, case reference number, payment transaction data (if applicable), eligibility responses, case statements, attestation,	To allow IDR to determine dispute eligibility under Article 21 DSA, review illegal content disputes, and issue non-binding decisions under Irish law.	Legitimate Interest: Meeting our statutory functions as a certified ODS body under the Digital Services Act (DSA). Consent: (For optional



case content, platform's statement of reasons, appeal statements, and metadata.		updates/communications).
Third-Party Data: Information posted on platforms, or posted about third parties, provided within a dispute submission.	To evaluate and handle illegal content disputes where third parties are named or implicated.	Legitimate Interest: Fulfilling our certified obligations under the DSA to resolve disputes brought before us.
Website & Analytics Data: IP address, browser type, operating system, visit frequency, session duration, referral URL, display settings.	To maintain Website security, ensure proper presentation, and analyse aggregate metrics.	Legitimate Interest: Strictly necessary functional cookies. Consent: Performance, functionality, and targeting cookies.
Stakeholder & Event Data: Name, email address, organization.	To manage registration and attendance for IDR events, seminars, or briefings.	Consent / Legitimate Interest: Facilitating event management.
Supplier & Platform Contacts: Staff names and business email addresses.	To receive goods/services and manage administrative relationships with platforms and vendors.	Legitimate Interest / Performance of Contract.

11. SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA

- 11.1. Due to the nature of illegal content disputes, cases submitted to IDR may inadvertently contain special category data (e.g., political opinions, religious beliefs) or criminal conviction/offence data. Where we process special category data, our legal basis is that processing is necessary for reasons of substantial public interest ([Article 9\(2\)\(g\) GDPR](#)) in performing our certified functions under the [Digital Services Act](#). Criminal conviction or offence data is processed strictly in accordance with The [Irish Data Protection Act 2018](#) and [Article 10 GDPR](#).

12. DISCLOSURE OF YOUR PERSONAL INFORMATION

- 12.1. Depending on your dealings with us, we may share some or all of the personal information we collect with the following external recipients:
- a) Online Platforms / Providers: We will share relevant case identifiers



(e.g., case reference numbers or content descriptions) with the platform provider involved in the dispute to facilitate investigation and settlement.

- b) Regulatory Bodies: We report dispute statistics and determinations to statutory regulators, such as Coimisiún na Meán and the European Commission, on an anonymised basis as required by Article 21 of the [DSA](#).
- c) Service Providers: Third parties providing hosting, case management tools, IT security, translation/text tools, back-office administration, and payment processing.

13. INTERNATIONAL TRANSFERS OF YOUR PERSONAL INFORMATION

13.1. Certain service providers or technology vendors may be based outside the European Economic Area (EEA). Whenever international transfers occur, we implement appropriate safeguards in compliance with applicable data protection laws, such as:

- a) Standard Contractual Clauses (SCCs) approved by the European Commission, supplemented by transfer impact assessments where necessary;
- b) Transfers to countries covered by an official European Commission adequacy decision.

14. RETENTION AND PROTECTION OF YOUR PERSONAL INFORMATION

14.1. We will not retain your personal information longer than necessary to fulfill the dispute settlement process, comply with legal and regulatory obligations, or resolve potential legal claims. Where data is no longer required, it is securely deleted or anonymized. Please refer to our [Data Retention Policy](#) for further information.

14.2. We maintain appropriate technical and organizational security measures designed to protect personal information against accidental loss, unauthorized access, or unlawful processing.

15. YOUR RIGHTS AND HOW TO EXERCISE THEM

15.1. Subject to statutory conditions and exceptions under the [GDPR](#) and [Data Protection Act 2018](#), you have the following rights regarding your personal information:

- a) Access: Request a copy of the personal information we hold about you.



- b) Rectification: Request correction of inaccurate or incomplete personal data.
- c) Erasure: Request deletion of your personal data where it is no longer required or processing is unlawful.
- d) Restriction: Request that we restrict processing under specific legal scenarios (e.g., pending accuracy checks).
- e) Portability: Request your personal data in a structured, machine-readable format.
- f) Objection: Object to processing based on legitimate interests.
- g) Withdraw Consent: Revoke consent at any time where processing relies on consent.
- h) Supervisory Authority: File a complaint with the Irish Data Protection Commission (DPC) or your local EU supervisory authority.