Data Retention Policy

Version 1.2. PDF (latest version) Last Updated: October 2026

1. PURPOSE

1.1. Impress Dispute Resolutions ("IDR", "we" or "us") is a Dublin-based out-of-court dispute settlement body, certified by Comisiún na Meán under Article 21 of the EU Digital Services Act.

1.2. IDR handles disputes between users and social media and content-sharing platforms concerning illegal content distributed, hosted, published or shared by those platforms. IDR therefore needs to use information, records and data on an everyday basis in order to carry out our business and operations. Those records and that information incudes personal data for the purposes of applicable data protection law.

1.3. On the basis that we are registered in Ireland and operate both in Ireland and the UK, the main applicable data protection laws are the General Data Protection Regulation ("GDPR") (both the EU- and UK-specific versions), the Irish Data Protection Act 2018 and the UK Data Protection Act 2018.

1.4. Given that the concept of personal data has such a broad definition – i.e. any information from which a living person may be identified, identified whether directly or indirectly – this means that we take on a broad range of obligations under applicable data protection law.

1.5. One of those obligations relates to data retention: we are only allowed to retain personal data as long as there is a good, valid and genuine organisational reason to do so. Non-exhaustive examples of good reasons are where we need to use the information for our casework or an IDR business or operational reason, compliance with applicable law or in the context of a potential or active legal dispute, for commercial or financial reasons or where use of personal data is in the public interest.

1.6. This data retention policy (and the supporting retention schedule annexed to it) sets out how we will comply with the data retention rules.

1.7. There are often good reasons why we need to keep personal data (because we would be unable to carry out our work effectively without it), and there are legal and regulatory requirements for us to retain certain information for specified periods. However, we are not allowed to retain personal data indefinitely or on a "just in case" basis, and retaining data can expose us to risks such as regulatory investigations and fines, court claims and damages awards, legal costs, allegations of criminal wrongdoing and reputational damage.

1.8. However, this retention policy is broader in scope than compliance with data protection law: good information governance and record-keeping management and hygiene practices are essential functions to a well-run organisation. Certain records (regardless of whether they contain personal data) need to be kept for certain legally mandated periods while certain records need to be kept so that we can provide our services effectively and efficiently.

2. SCOPE OF POLICY

2.1. This policy applies to all IDR work and operations and covers all data that we hold, have control over or have access to. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

2.2. This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that we are responsible for but is held by staff members on personal devices.

2.3. This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, records of unlawful or illegal content or conduct personal data and non-personal data. It also gives guidance on how we classify our data.

2.4. This policy applies to all our departments, units and functions in both Ireland and the UK.

2.5. Failure to comply with this policy can expose us to fines and penalties, court claims, allegations of criminal wrongdoing adverse publicity, and more broadly difficulties in providing our services given that these depend on the receipt, creation, storage and disclosure of records. In particular it may interfere with, undermine or prejudice our ability or entitlement to handle the disputes which are sent to us for resolution.

2.6. This policy does not form part of any staff member's contract for work or services, and we may amend it at any time. Nonetheless, failure to comply with this policy may be deemed a disciplinary offence, depending on the circumstances and consequences.

3. GUIDING PRINCIPLES

3.1. Through this policy, and our data retention practices, we aim to meet the following commitments:

a) We comply with all legal and regulatory requirements relating to the retention of data.
b) We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
c) We handle, store and dispose of data responsibly and securely.
d) We create and retain data where we need this to operate IDR effectively and to provide our services, but we do not create or retain data without good reason.
e) We allocate appropriate resources, roles and responsibilities to data retention.
f) We regularly remind employees of their data retention responsibilities.
g) We regularly monitor and audit compliance with this policy and update this policy when required.

4. ROLES AND RESPONSIBILITIES

4.1. Responsibility of all staff and individuals working on behalf of or providing services to IDR:

a) We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practice.
b) All staff and individuals working on behalf of / providing services to IDR must comply with this policy, the Record Retention Schedule, any communications suspending

data disposal and any specific instructions from our Data Protection Lead who has ultimate responsibility for data retention issues.

c) An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination.

d) It is therefore the responsibility of everyone to understand and comply with this policy.

4.2. We have designated the Data Protection Lead [Lexie Kirkconnell-Kawana, please contact her at info@impressdisputeresolutions.org] as the person in charge of applying and enforcing this policy.

4.3. The Data Protection Lead is responsible for the following (in consultation with the Directors):

a) Identifying the data that we must or should retain, and determining, the proper period of retention.

b) Arranging for the proper storage and retrieval of data, co-ordinating with outside suppliers where appropriate and additionally, handling the destruction of some records whose retention period has expired.

c) Administering and applying the requirements of this policy in practice.

d) Helping department heads implement the requirements of this policy (and related best practices) in practice.

e) Monitoring and enforcing compliance with the requirements of this policy.

f) Providing guidance, training, monitoring and updating in relation to this policy.

5. TYPES OF DATA AND DATA CLASSIFICATIONS

5.1. **Case files**: bearing in mind the nature of the services which IDR provides, the main types of records which we generate in doing our work are our case files. In overview, and non-exhaustively, these include the following types of information and records:

a) Claimant identities, contact details, details of complaint, original webform submission and reason for using our services, general correspondence and eligibility check and admissibility assessment records.

b) Details of organisations who refer a case on a claimant's behalf (and our contacts / liaisons at those organisations).

c) Details of third-party individuals and/or organisations depicted or discussed in the disputed content or related allegations of unlawful or illegal conduct (i.e. the person or organisation accused of wrongdoing in the applicable case).

d) Platform notification, scheme agreement and platform engagement forms.

e) Social media or content-sharing platforms with whom we work to settle disputes and correspond where (and our contacts / liaisons at those organisations).

f) Details of our case administrators and decision-makers who work on each case, including their appointment records, any conflict of interest, qualifications and experiences, analyses or opinions on particular cases or matters, case assessments, evidence gathering records, written decisions and supporting logic.

g) Case flow or management records, detailed information on how each case progresses.

h) Dispute intake and case creation, triage and completeness check.

i) Remedy tracking and decision / recommendation implementation monitoring records.

j) Service review forms / records of individual complaints.

5.2. **Records of illegal and unlawful (including allegedly illegal and unlawful) content** – given that IDR's purpose is to handle and resolve disputes between social media and content-sharing platforms and their users concerning illegal and unlawful content, IDR is likely to hold records

which reflect or evidence illegal or unlawful conduct. We are not legally prohibited from holding this, but we do need to ensure that such records are held only so long as a complaint, case or applicable appeal period is live. Examples of such content include hate speech, bullying, violence, non-consensual intimate images, misinformation and material which is or amounts to defamatory, intellectual property infringement, misuse of private information, and breach of data protection rights or duties of confidence.

5.3. **Formal or official records.** Some records and the data contained in them are particularly important to us because they serve a formal or legal purpose. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions or our services provided, or because it is important to the running of our organisation. Please see below for more information on retention periods for this type of data.

5.4. This includes formal legal (e.g. corporate registration or structure records or eligibility check records, records of cases taken on in case these progress to full legal disputes), regulatory (e.g. data protection compliance documents such as our record of processing activities and data protection policy) and policy / procedural documents (e.g. ODS procedural rules, our decision-making framework and HR policy documents).

5.5. **Disposable information.** Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Record Retention Schedule. Examples may include:

a) Duplicates of originals that have not been annotated.
b) Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
c) Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Impress Dispute Resolutions Ltd and retained primarily for reference purposes.
d) Ordinary routine and administrative correspondence.
e) Marketing and promotional material (sent and received).
f) Spam and junk mail.

5.6. **Information collected from our website.** Completed webforms and information collected by cookies and similar technologies when individuals visit our use our website. Details of the types of cookies and other technologies we use, and information collected by those cookies and other technologies is set out in our Cookie Policy.

5.7. **Personal data.** All of the types of records and information listed above may contain or constitute personal data (as defined above). The main obligations relating to data retention are set out in data protection law – given that most of our records contain or amount to personal data, the rules set out below are designed with a view to complying with those data retention obligations.

5.8. **Confidential information relating to IDR or others.** Confidential information is any data, record or material which is particularly private, secret or sensitive, either innately due to its own nature or due to the circumstances in which we hold or receive it. For example, information which amounts to evidence that somebody is guilty or liable of illegal or unlawful conduct is naturally more sensitive (because unauthorised disclosure of or access to such information would put them at clear risk of adverse impact).

5.9. Where information is confidential and in our custody, we owe a legally enforceable duty of

confidence (i.e. legal requirement to keep secret or private) as between IDR and the relevant person or organisation. Confidential information may only ever be disclosed outside IDR where authorised by the Data Protection Lead. Unsolicited confidential information submitted to us, or information which is confidential but is not necessary for a case we are working on or related to any case we are working on, should be refused, returned to the sender where possible, and deleted.

5.10. **Financial information.** IDR keeps financial records (e.g. payment card or account details, transaction records) relating to payment for the provision of our services or payments relevant to the outcome or resolution of a matter (e.g. any fees to settle a dispute in exchange for a waiver of legal rights to pursue a court claim).

5.11. **Statistical / anonymised information.** We create and generate our own statistical and trend / pattern / impact assessment and analysis records and information. Some of this is generated to comply with applicable regulatory or legislative requirements, some is created for our own internal purposes (e.g. reviewing the impact and effectiveness of our work with a view to improvement or expanding access). This information is not personal data (because no living individual can be identified from it).

5.12. This information includes:

a) Comisiún na Meán minimum requirements
   i. Number of disputes received
   ii. Types of disputes
   iii. Outcomes of disputes
   iv. Average time taken to resolve or settle disputes
   v. Any complaints, shortcomings or difficulties encountered

b) European Commission minimum requirements
   i. Annual dispute numbers per organization
   ii. Outcomes
   iii. Average resolution time
   iv. Identifying systemic or sectoral shortcomings
   v. Identifying best practices
   vi. Recommendations for improvement

c) Platform transparency minimum requirements
   i. Number of disputes submitted to ODS bodies
   ii. Outcomes
   iii. Median time to complete procedures
   iv. Share of disputes where the relevant platform implemented the ODS body's decision

6. RETENTION PERIODS

6.1. **Case files.** While there are different legal limitation periods (i.e. the statutory time period in which you are entitled to bring a legal claim arising out of the applicable circumstances) which apply to the different types of claim which we handle, as a general rule we keep our case files live on our systems for 6 years from the point at which our involvement in a matter finishes or we stop providing our services. This is because individuals technically have the right to bring a legal claim against us for 6 years from that point (or 6 years from a specific act or omission by us, if this is what is specifically claimed about).

6.2. In turn this means that we keep case file records for the full length of all applicable statutory time periods, should our records be required to be disclosed in the context of a formal court claim.

6.3. With the above said, in some situations parties to a dispute may genuinely need to access and use records outside of this guideline retention period (for example in cases of latent damage or serious criminal investigations). Where this is the case, once the standard 6-year retention period ends, we put the relevant case file records into a secure archive which can only be accessed by a restricted circle of senior personnel. This takes documents beyond the live and daily access and use of IDR, but IDR but retains a copy behind strict need-to-know access protocols in case of genuine need. Please see below for more details about secure archiving.

6.4. There are some types of criminal conduct which we will be asked to investigate which has no applicable legal limitation period (because they are considered sufficiently serious to justify this, e.g. hate speech). However, given that allegations of serious criminal wrongdoing are innately sensitive, private and confidential, and given additional protection under data protection law, IDR's policy is to place such records in secure archive after the 6-year retention period elapses as an additional information security and data-protective measure.

6.5. **Records of illegal / unlawful conduct.** Because these records are normally at the heart of the relevant case files, the same retention periods specified above apply here.

6.6. **Formal or official records.** Any data that is part of any of the categories listed in the Record Retention Schedule contained in the Annex to this policy, must be retained for the amount of time indicated in the Record Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, or if you believe an exception should be made to allow a record to be retained for longer than the amount of time indicated in the Record Retention Schedule, please contact IDR at info@impressdisputeresolutions.org.

6.7. **Disposable information.** The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for genuine operational purposes. Once it no longer has any operational purpose or value it should be securely disposed of.

6.8. **Information collected from our website.** Webform submissions will be retained for the same guideline periods as set out in relation to casefiles above (because they are usually the starting point of the cases which we manage with a view to resolution). Please see the cookie / other web technology duration periods set out in our Cookie Policy for specific information about storage of information collected by cookies or other technologies.

6.9. **Personal data.** As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data. If we do not need to retain personal data for the resolution of a case or in case of possible legal proceedings, then it should be deleted before the usual 6-year retention period elapses.

6.10. **Confidential information.** Similar to the position relating to personal data, confidential information should only be kept as long as there is a genuine IDR organisational or operational need to hold it. If confidential information is not genuinely necessary to the resolution of a case or to possible legal proceedings, then it should be deleted before the usual 6-year retention period elapses for a case file.

6.11. **Financial information** (banking details, credit card details etc) about supporters. Please see the applicable guideline retention period in the Record Retention Schedule.

6.12. **Statistical / anonymised information.** While some of these records are considered business confidential for IDR, as these records do not contain or amount to personal data then the data retention obligations set out in data protection law do not apply. Given that individual case details cannot be gleaned from this information alone, and most of these records are required by virtue of regulatory or legal obligations, it is usually acceptable to keep these on an open-ended basis (i.e. as long as IDR is a going concern).

6.13. What to do if data is not listed in the Record Retention Schedule. If data is not listed in the Record Retention Schedule, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Record Retention Schedule, or if you are unsure, please contact the Data Protection Lead at info@impressdisputeresolutions.org.

7. STORAGE, BACK-UP AND ARCHIVING

7.1. **Storage**. Our data must be stored in a safe and secure manner and subject to need-to-know access protocols only. All records in IDR's custody are kept subject to our usual technical (i.e. software / electronic) and organisational (physical / office-based) security measures.

7.2. In the main, IDR's records are stored on the following principal systems:

a) HubSpot (our case management system)
b) Microsoft SharePoint (our case file storage system)
c) Our WordPress website which hosts forms and public information

7.3. IDR records and information should only be stored on IDR devices, systems or drives. IDR records or information must not be stored on personal devices, networks or systems.

7.4. **Back-ups.** Back-up records are kept to ensure retention and accessibility of key operational information in case of loss, theft or disaster. Back-up records are not kept as a circumvention of or exception to ordinary retention periods: the same retention periods which apply to main records also apply to back-ups (because we are only needed to keep a back-up as long as there is an organisational or operational need for a record or document).

7.5. As a general rule, we apply the following approach to back-ups:

a) Daily backups – keep for 30 days for quick fixes like restoring deleted or lost files or fixing recent errors.
b) Weekly backups – keep for 12 weeks to catch older, undetected issues like malware, unauthorised access or data corruption.
c) Monthly backups – keep for 12 months for end-of-year or seasonal reviews, long-term historical recovery or audits.
d) Yearly backups – should be kept no longer than the applicable retention period set out below.

7.6. **Secure archiving.** In certain situations (e.g. where we hold evidence of / information relevant to serious criminal wrongdoing, where the applicable legal limitation period is longer than 6 years, in case where we think there is the potential for latent damage or where information is important and we are genuinely not yet able to decide whether information can safely be deleted or not) then it is permissible to put records into a "secure archive".

7.7. This means that the relevant record is taken out of the live, daily use and access of IDR personnel and is stored in a location which can only be accessed by a restricted circle of senior personnel including the Data Protection Lead and behind strict need-to-know access protocols. Access will then only be granted on specific request and where such requests are reviewed and agreed by those senior personnel who control access, provided they agree that there is a genuine and good organisational need to re-access the information.

7.8. Information in secure archive cannot be held open-endedly or indefinitely as a way to circumvent data retention rules: the secure archive will be checked periodically (at least annually) to consider whether there is still a genuine and good organisational reason to keep the information, even in a format which is put beyond the daily and live reach and access of IDR personnel.

7.9. **Deletion, destruction and disposal.** Where a record is to be deleted, destroyed or disposed of (as applicable) in compliance with this policy, then such deletion, destruction or disposal must be secure, permanent and irretrievable.

7.10. For paper records:

a) Information not containing personal data or confidential information can be placed in normal recycling bins without further treatment.
b) Information containing personal data, confidential information or anything to do with a case we have worked on should be destroyed by shredding or pulping prior to being recycled.

7.11. Electronic records should be deleted or destroyed in a manner which is non-recoverable even if data search or recovery techniques are used to carry out a search for that data. Electronic equipment which is decommissioned from IDR use (e.g. to be recycled in case of upgrade or returned at the end of the lease) should be wiped or reset to original factory settings prior to being taken out of IDR control). Deletion of electronic records and decommissioning of electronic equipment should always be co-ordinated with IT Support.

7.12. The destruction, deletion or disposal of data or records must stop immediately upon notification from the Data Protection Lead that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see 8.1.). Destruction may begin again once the Data Protection Lead lifts the requirement for preservation.

8. SPECIAL CIRCUMSTANCES

8.1. Preservation of documents for contemplated litigation and other special situations. All IDR personnel should note the following general exception to any stated destruction schedule: If you believe, or Data Protection Lead informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government or regulatory investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the Data Protection Lead determines those records are no longer needed. Preserving documents includes suspending any requirements in the Record Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

8.2. To be clear, once a claimant or respondent asks us to preserve information for litigation hold or indicates an intention to commence litigation, it is permissible to keep records longer than the periods set out in the Retention Schedule for as long as the relevant litigation or dispute (and any applicable appeal periods) remain active.

8.3. If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Data Protection Lead at info@impressdisputeresolutions.org.

8.4. In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

9. WHERE TO GO FOR ADVICE AND QUESTIONS

9.1. Any questions about this policy, the retention rules or guideline retention periods we apply which are relevant to your function or department should be raised with the Data Protection Lead, who is in charge of administering, enforcing, and updating this policy.

10. BREACH REPORTING AND AUDIT

10.1. **Reporting policy breaches**. We are committed to enforcing this policy as it applies to all forms of data. The effectiveness of our efforts, however, depend largely on IDR personnel. If you feel that you or someone else may have breached this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with the Data Protection Lead. If you do not report inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.

10.2. No one will be subject to, and we do not, allow any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.

10.3. **Audits**. The Data Protection Lead will periodically review this policy and its procedures (including where appropriate by taking outside legal or auditor advice) to ensure we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

ANNEX 1: RETENTION SCHEDULE

As is set out in this Policy, records, information and data should only be kept for as long as genuinely required to meet the operational needs of IDR, together with any legal and regulatory requirements we must adhere to.

Records are assessed to establish their necessity and their importance and value as a source of information about IDR and its operations, relationships and environment and whether there are any legal or statutory retention periods that must be adhered to.

This retention scheduler forms a key part of the management of data, information and records held by IDR and records the predetermined retention periods for those documents.

Information and records held by IDR will be subjected to one of the following outcomes:

- Destroy or delete after retention period expires.
- Temporary extension – a record can be retained for longer than the guideline retention period with the written authorisation of the Data Protection Lead where there is still a genuine organisational, operational or legal reason to do so (for example where an individual has commenced legal proceedings which are active beyond our usual guideline retention period).
- Permanently preserved – certain categories of records are capable of being permanently preserved, for example because of the seriousness of the wrongdoing they reveal, in case of latent damage which may arise from the relevant circumstances or because they do not contain personal data or confidential information.
- Secure archiving for subsequent review – where our guideline retention period has expired but there is a longer applicable statutory retention period, where contents are particularly sensitive, private or confidential or where information is particularly important and we cannot yet decide whether to delete.

Review and application of this policy

IDR shall carry out an annual review of the records it holds and delete any records, information or data where it is no longer justifiable to retain it. Deletion, disposal or destruction shall be effected as soon as is reasonably practicable after decisions to delete are made, and in any case no longer than one month after retention of the relevant record, information or data was identified as no longer justified.

Guideline retention periods

IDR applies the following guideline retention periods to the following types of records which it holds.

Financial information

Document	Guideline Retention Period	Reason	Action at end of retention period
Bank records	7 years from the end of the relevant financial year	By reference to applicable legislation such as in the UK the Companies Act 2006/Taxes Management Act	Secure disposal, deletion or destruction.
Remittance advices, invoices, payment records			
Correspondence regarding fees and			

payment		1970/HMRC/ Revenue Commissioners	
Receipts cash book	10 years.		
Sales ledger			

Purchase Invoices and Supplier Documentation

Document	Guideline Retention Period	Reason	Action at end of retention period
Payments cash book or record of payments made	7 years from the end of the relevant financial year	By reference to applicable legislation such as in the UK the Companies Act 2006 and HMRC/ Revenue Commissioners	Secure disposal, deletion or destruction.
Purchase ledger			
Invoices			
Petty cash records			

Case records

The retention period and treatment which we apply depends on the type of applicable criminal offence or unlawful conduct (alleged or substantiated) which forms the subject matter of the relevant case file.

Document	Guideline Retention Period	Reason	Action at end of retention period
Defamation	6 years from expiry or termination of IDR's services or involvement	The statutory limitation period for a defamation claim in both Ireland and the UK is 1 year from the publication of the relevant statement, so a 6-year retention period covers the period in which a service user can bring a claim against IDR and will be enough to cover any litigation which may arise.	Secure disposal, deletion or destruction, unless litigation has been or is likely to be commenced against us within the 6-year limitation period, in which case the material can be kept until the relevant litigation, or dispute has been resolved (including any applicable appeal periods).
Breach of data protection law / infringement of data protection rights	6 years from expiry or termination of IDR's services or involvement	The statutory limitation period for a claim under data protection law in the UK and Ireland is 6 years from the relevant event or incident which is said to infringe data protection law, so a 6-year period from termination or expiry	Secure disposal, deletion or destruction unless formal litigation has been commenced or is likely to be commenced (whether involving IDR as a party or otherwise) during either of the applicable limitation periods, in which case the material

		of our services will cover both applicable limitation periods (i.e. to make a claim against IDR and to make a claim under data protection law).	can be kept until the relevant litigation or dispute has been resolved (including any applicable appeal periods).
Misuse of private information	6 years from expiry or termination of IDR's services or involvement	The statutory limitation period for a claim in misuse of private information in the UK and Ireland is 6 years from the relevant event or incident, so a 6-year retention period from termination or expiry of our services will cover both applicable limitation periods (i.e. to make a claim against IDR and to make a claim under data protection law).	Secure disposal, deletion or destruction unless formal litigation has been commenced or is likely to be commenced (whether involving IDR as a party or otherwise) during either of the applicable limitation periods, in which case the material can be kept until the relevant litigation or dispute has been resolved (including any applicable appeal periods).
Breach of confidence claims	6 years from expiry or termination of IDR's services or involvement	The statutory limitation period for claim for breach of confidence in the UK is 6 years from the relevant event or incident which is said to be a breach of confidence. The same retention period applies in Ireland, but the court retains a discretion to allow a claim to be brought in circumstances where it considers it equitable to do so. A 6-year retention period from the end of our involvement will therefore cover most litigation / dispute uses but may need to be extended in certain circumstances.	Secure disposal, deletion or destruction unless formal litigation has been commenced or is likely to be commenced (whether involving IDR as a party or otherwise) during either of the applicable limitation periods, in which case the material can be kept until the relevant litigation or dispute has been resolved (including any applicable appeal periods). If we do not know of any litigation being commenced within the 6-year period, case files for beach of confidence claims should be put in secure archive in case they come to be needed in Irish litigation where a court considers it equitable

			to allow a claim to be brought outside the limitation period. There is no set period at which such records must or should be deleted, but we recommend deleting from secure archive after a total period of 25 years from the end of our involvement as a longstop deletion date after which it is unlikely that a claim would be brought or permitted.
Infringement of intellectual property rights	6 years from expiry or termination of IDR's services or involvement	The statutory limitation period for an IP infringement claim in the UK and Ireland is 6 years from the relevant event or incident, so a 6-year retention period from termination or expiry of our services will cover both applicable limitation periods (i.e. to make a claim against IDR and to make a claim under data protection law).	Secure disposal, deletion or destruction unless formal litigation has been commenced or is likely to be commenced (whether involving IDR as a party or otherwise) during either of the applicable limitation periods, in which case the material can be kept until the relevant litigation or dispute has been resolved (including any applicable appeal periods).
Hate speech	6 years from expiry or termination of IDR's services or involvement	There is no statutory limitation period for the prosecution of hate speech crimes in the UK or Ireland unless the matter is being investigated or tried as a minor or summary offence, in which case the limitation period is 6 months for the CPS or Garda Síochána to institute proceedings. A 6-year period therefore covers the limitation period in which a service user can bring a claim against IDR arising	For minor / summary offences where the CPS or Garda Síochána have contacted us already, secure disposal, deletion or destruction at the end of the 6-year retention period unless we know that the relevant investigation or proceedings remain active (including any appeal periods). If the facts are more serious and we have not been contacted by the CPS or Garda Síochána (or any

		from the provision of our services, in which case we will be contacted by either the CPS or Garda Síochána before the end of the retention period if the matter is to be prosecuted as a minor or summary offence.	individuals involved) indicating that the matter will be prosecuted as a minor or summary offence, then the case file should be moved into secure archive on expiry of the retention period and preserved indefinitely in case the matter ever comes to be prosecuted or in case of latent damage (because no statutory limitation period applies).
Offences relating to creation or sharing of non-consensual indecent or explicit images	6 years from expiry or termination of IDR's services or involvement	In the UK perpetrators can be prosecuted for up to 3 years after the offence occurred, and there is a 6-year limitation period for civil claims which arise from the same fact (i.e. where a victim wants to sue the perpetrator). In Ireland the applicable prosecution limitation period is 2 years, and the same 6-year limitation period for civil claims applies. A retention period of 6 years from the end of our involvement therefore covers us for all applicable statutory limitation periods.	Secure deletion, disposal or destruction unless we know or have credible grounds to suspect that any proceedings are active or likely (including any appeal periods). With that said, where continued retention beyond 6 years is justified because of active or likely criminal / civil proceedings, on expiry of the 6-year retention period material should be moved to secure archive as an additional data security measure (because this content will always be highly sensitive, private and confidential), where it will be subject to annual review until it is deleted when there is no plausible reason to retain it related to active or live proceedings.
Bullying and violence	6 years from expiry or termination of IDR's services or involvement	The standard limitation periods for civil claims arising out of threatened or actual	For minor / summary offences where the CPS or Garda Síochána have contacted us already,

		violence are 3 years in the UK and 6 years in Ireland, but these can be extended in particularly severe circumstances where a court considers it equitable to do so. The applicable statutory limitation periods for criminal offences related to violence are 6 months for minor offences in both jurisdictions and there are no limited for serious violence offences.	secure disposal, deletion or destruction at the end of the 6-year retention period unless we know that the relevant investigation or proceedings remain active (including any appeal periods). If the facts are more serious and we have not been contacted by the CPS or Garda Síochána (or any individuals involved) indicating that the matter will be prosecuted as a minor or summary offence, then the case file should be moved into secure archive on expiry of the retention period and preserved indefinitely in case the matter ever comes to be prosecuted or in case of latent damage (because no statutory limitation period applies).

Governance/Contracts

Document	Guideline Retention Period	Reason
Board minutes (trustees/directors) of meetings and decisions	Permanently	By reference to applicable legislation such as the UK Companies Act 2006 requires these to be kept for at least ten years from the date of the meeting or decision, IDR policy is to keep these records permanently.
Annual accounts and reports	Permanently	By reference to the applicable legislation such as in the UK the Companies Act 2006 / HMRC/ Revenue Commissioners requires us to keep these for a minimum of 6 years, but IDR policy is to keep these records permanently.

Major agreements of significance to IDR	Permanently	HMRC / Revenue Commissioners; documents contain no personal data (other than e.g. name / title / position of signatory).
Investment certificates and records	Permanently	HMRC / Revenue Commissioners; documents contain no personal data (other than e.g. name / title / position of signatory).
Contracts with suppliers or agents, licensing agreements, rental/hire purchase agreements, indemnities and guarantees and other agreements or contracts which are not major agreements of significance to IDR	7 years after expiry or termination of the contract. If the contract is executed as a deed, 12 years.	HMRC / Revenues Commissioners

Registration / data protection compliance records for DPC in Ireland and DPO in UK

Document	Guideline Retention Period	Reason
Data protection: Registration certificates, legitimate interests' assessments, data protection impact assessments, record of processing activities, data retention policy, privacy policy, cookie policy, website terms of use	As long as IDR is a going concern	Necessary to demonstrate compliance with applicable data protection law, which will apply to IDR as long as we provide our services.
Policies	3 years after lapse	IDR Policy.
Employer's Liability insurance records (certificate and policy documents)	Permanently	Potentially of use as long as IDR is a going concern.
Accident reports and relevant correspondence	At least 3 years after the report was made if a UK incident, at least 10 years after the report was made if in Ireland.	Sch. 1, Part II, Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (UK), Reporting of Accidents and Dangerous Occurrences Regulations 2016 (Ireland)
Contracts with suppliers or agents, licensing agreements, rental/hire purchase agreements, indemnities and guarantees and other agreements or contracts which are not major agreements of significance to IDR	7 years after expiry or termination of the contract. If the contract is executed as a deed, 12 years.	HMRC / Revenues Commissioners

CCTV

Document	Guideline Retention Period	Reason	Action at end of retention period
CCTV Footage	One month	This is the guideline period recommended by the ICO in the UK	Secure deletion, disposal or destruction unless CCTV footage is

		and the Data Protection Commission in Ireland.	still required (e.g. in the context of an investigation, complaint or legal dispute), in which case retain until no longer required.

Statistical / anonymised information. Anonymised and aggregated information, including statistics and trend analysis, can be kept indefinitely because the contents do not amount to personal data (and therefore the data retention rules do not apply as they do to documents containing or amounting to personal data). This rule applies the same for documents created for internal use or for compliance with Comisiún na Meán, European Commission or platform transparency requirements.