Data Retention Policy

Revision History

Version	***Revision Date***	***Revised by***	***Section Revised***
1.0	15-SEP-2020	Rob Shelvey	Initial Draft
1.1	30-SEP-2020	Rob Shelvey	Updated Retention Register

Document Control

Document Owner:	***Version:***	***Status:***	***Date Approved:***
Dan Ni	V1.1	Live Policy	30-SEP-2020
Security Classification:	***Next Review Date:***		**Approved By:**
Low	01-SEP-2021		Dan Ni

Contents

Policy Statement

Scraper API recognises and understands that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the organisation.

This policy and related documents meet the standards and expectations set out by contractual and legal requirements and have been developed to meet the best practices of business records management, with the direct aim of ensuring a robust and structured approach to document control and systems.

Effective and adequate records and data management is necessary to: -

- Ensure that the business conducts itself in a structured, efficient and accountable manner
- Ensure that the business realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Support core business functions and providing evidence of conduct and the appropriate maintenance of associated tools, resources and outputs to clients and regulator
- Meet legislative, statutory and regulatory requirements
- Deliver services to staff and stakeholders in a consistent and equitable manner
- Assist in document policy formation and managerial decision making
- Provide continuity in the event of a disaster
- Protect the interests of the organisation and the rights of employees, clients and present and future stakeholders
- Protection personal information and data subject rights
- Avoid inaccurate or misleading data and minimise risks to personal information

Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles. Scraper API only ever retain records and information for legitimate business reasons and use and comply fully with the EU data protection laws and guidance.

Purpose

The purpose of this document is to provide Scraper API a statement of intent on how it provides a structured and compliant data and records management system with records being defined as all documents, regardless of the format, which facilitate the business activities and which are thereafter retained to provide evidence of its transactions or activities.

Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

It constitutes a series of integrated systems related to the core processes of the organisation which ensure that evidence of, and information about, its activities and transactions are captured and maintained as viable records. Unless otherwise specified the Data Retention Policy refers to both hard and soft copy documents.

Scope

The policy relates to all Scraper API staff *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with Scraper API)* within the organisation and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

General Data Protection Regulation (GDPR)

Scraper API needs to collect personal information about the people we employ, work and deal with to effectively and compliantly carry out our everyday business functions and activities and to provide the products and services defined by our business type. This information can include *(but is not limited to),* name, address, email address, phone numbers, photographs, and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the ***General Data Protection Regulation***, Irish data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Retention Policy and processes comply fully with the GDPR's fifth Article 5 principle: -

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation').***

Objectives

A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions. It is Scraper API's objective to implement the necessary records management procedures and systems which assess and manage the following processes: -

- The creation and capture of records
- Compliance with legal, regulatory and contractual requirements
- The storage of records
- The protection of record integrity and authenticity
- The use of records and the information contained therein
- The security of records
- Access to and disposal of records

Records contain information that are a unique and invaluable resource to Scraper API and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

Scraper API objectives and principles in relation to Data Retention & Records Management are to: -

- Ensure that Scraper API conducts itself in an orderly, efficient and accountable manner
- Realise best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Support core business functions and providing evidence of conduct and the appropriate maintenance of associated tools, resources and outputs to clients and 3rd parties
- Meet legislative, statutory and regulatory requirements
- Deliver services to staff and stakeholders in a consistent and equitable manner
- Provide continuity in the event of a disaster
- Protect the interests of the organisation and the rights of employees, clients and present and future stakeholders
- Ensure the safe and secure disposal of confidential data and information assets
- Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each body's rules or terms.
- Ensure that no document is retained for longer than is legally or contractually allowed
- Mitigate against risks or breaches in relation to confidential information

Guidelines & Procedures

Scraper API manages records efficiently and systematically, in a manner consistent with the GDPR requirements, ISO15489 and regulatory Codes of Practice on Records Management. This policy is widely disseminated to ensure a standardised approach to data retention and records management.

Records will be created, maintained and retained in order to provide information about and evidence of Scraper API transactions, customer, employment and activities. Retention schedules will govern the period that records will be retained and can be found in the ***Record Retention Periods*** table at the end of this document.

It is our intention to ensure that all records and the information contained therein is: -

- **Accurate** - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- **Accessible** - records are always made available and accessible when required (*with additional security permissions for select staff where applicable to the document content*)
- **Complete** - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document

- **Compliant** - records always comply with any record keeping legal and regulatory requirements
- **Monitored** – staff, company and system compliance with this Data Retention Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

Retention Period Protocols

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All company and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

For all data and records obtained, used and stored within Scraper API, we: -

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
- Establish periodical reviews of data retained
- Establish and verify retention periods for the data, with special consideration given in the below areas: -
    - the requirements of Scraper API
    - the type of personal data
    - the purpose of processing
    - lawful basis for processing
    - the categories of data subjects
- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, Scraper API will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices
- Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered
- Transfer paper based records and data to an alternative media format in instances of long retention periods (*with the lifespan of the media and the ability to migrate data where necessary always being considered*)

Designated Owners

All systems and records have a designated owner, known as **Information Asset Owners (IAO)** throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, business area and level of access to data required. The designated owner is recorded on the Retention Register and is fully accessible to all employees. Data and records are never to be reviewed, removed, accessed or destroyed with the prior authorisation and knowledge of the designated owner.

Document Classification

Scraper API have detailed Asset Management protocols for identifying, classifying, managing, recording and coordinating Scraper API assets (*including information*) to ensure their security and the continued protection of any confidential data they store or give access to. We utilise a ***data map to*** document and categorise the

assets under our remit and carry out regular Information Audits to identify, review and document all flows of data within Scraper API.

The Information Audit enables us to identify, categorise and record all personal information obtained, processed and shared by our company in our capacity as a controller and processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Retention periods

Our information audits and registers enable us to assign classifications to all records and data, thus ensuring that we are aware of the purpose, risks, regulations and requirements for all data types.

We utilise 5 main classification types: -

1. **Unclassified** - information not of value and/or retained for a limited period where classification is not required or necessary
2. **Public** - information that is freely obtained from the public and as such, is not classified as being personal or confidential
3. **Internal** - information that is solely for internal use and does not process external information or permit external access
4. **Personal** - information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws
5. **Confidential** - private information or systems that must be secured at the highest level and are afforded access restrictions and high user authentication

The classification is used to decide what access restriction needs to be applied and the level of protection afforded to the record or data. The classification along with the asset type, content and description are then used to assess the risk level associated with the information and mitigating action can then be applied.

Suspension of Record Disposal for Litigation or Claims

If Scraper API is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our firm, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

Storage & Access of Records and Data

Documents are grouped together by category and then in clear date order when stored and/or archived. Documents are always retained in a secure location, with authorised personnel being the only ones to have

access. Once the retention period has elapsed, the documents are either reviewed, archived or confidentially destroyed dependant on their purpose, classification and action type.

Expiration of Retention Period

Once a record or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR requirements or to archive records for a further period.

Destruction and Disposal Of Records & Data

All information of a confidential or sensitive nature on paper or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

Scraper API is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

Paper Records

Scraper API will utilise Onsite-Shredding or A Professional Shredding Service Provider to dispose of all paper materials.

Employee shredding machines and confidential waste sacks are made available throughout the building and where we use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

Electronic & IT Records and Systems

Scraper API uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information processed and held of these whilst they are active, this disposal must be handled in an ethical and secure manner.

The deletion of electronic records must be organised in conjunction with the IT Department who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal in details must be provided to the designated owner to maintain an effective and up to date a register of destroyed records.

Only the IT Department can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department personally. Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

In all disposal instances, the IT Department must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the IT Department is responsible for liaise with the information Asset Owner and updating the Information Asset Register for the asset that has been removed.

It is the explicit responsibility of the asset owner and IT Department to ensure that all relevant data has been sufficiently removed from the IT device and backed up before requesting disposal and/or prior to the scheduled pickup.

Internal Correspondence and General Memoranda

Unless otherwise stated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support (i.*e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed*).

Where correspondence or memoranda that do not pertain to any documents having already be assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases or at a maximum, 2 years.

Examples of correspondence and routine memoranda include (but are not limited to): -

- Internal emails
- Meeting notes and agendas
- General inquiries and replies
- Letter, notes or emails of inconsequential subject matter

Compliance and Monitoring

Scraper API are committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

Responsibilities

Heads of departments and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure that the records created, received and controlled within the purview of their department, and the systems (*electronic or otherwise*) and procedures they adopt, are managed in a way which meets the aims of this policy.

Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with Scraper API protocols.

Retention Periods

The following section of this document contains our regulatory, statutory and business retention periods and the subsequent actions upon reaching said dates. Where no defined or legal period exists for a record, the default standard retention period for legal purposes is 7 years.

Retention Register

RECORD	RETENTION PERIOD	ASSET OFFICER	ACTION	NOTES
Information, data or record	*Period for retaining record & accompanying notes*	*Who is responsible for reviewing periods*	*Destroy, archive, review etc*	
Sign Up	Until account closure		Destroy	
Sales Forms	2 years		Review	
Email	2 years		Review	Review emails older than 2 years and delete if no longer required
Customer Support Data	2 years		Review	
Payments/Invoices	2 years		Review	
Customer Data	2 years		Review	