# ISMS DATA PROTECTION AND PRIVACY POLICY (GDPR)

**Introduction**
The General Data Protection Regulations regulate the processing of information relating to individuals, this includes the obtaining, holding, using, or disclosing of such information, and covers computerised records as well as manual filing systems and card indices. Rapidity is registered with the ICO as a data processor.

Rapidity will hold the minimum personal information necessary to enable it to perform its functions. All such information is confidential and needs to be treated with care, to comply with the law.

All jobs that contain data will be risk assessed using the Security Classification Risk Assessment and identified as High, Medium, or Low, which will identify the level of security applied.

**Summary of Principles**
Data users must comply with the Data Protection principles of good practice which underpin the Act these state that personal data shall:

1. Be obtained and processed fairly and lawfully (that the subject of the data has consented to its collection and use.)
2. Be held only for specified purposes
3. Be adequate and relevant but not excessive
4. Be accurate and kept up to date.
5. Be held for no longer than necessary
6. Be accessible to data subjects.
7. Be subject to the appropriate security measures.
8. Not be transferred outside the EEA (European Economic Area with includes the EU member states: Austria, Belgium, Denmark, Eire, Finland, France, Germany, Greece, Italy, Luxembourg, Netherlands, Portugal, Sweden & the UK as well as Iceland, Liechtenstein, Norway, and Switzerland)

Rapidity and all its staff who process or use personal data must ensure that they always abide by these principles. This policy has been developed to ensure this happens.

**Requirements of the Act**
Rapidity staff must identify any filing system or computer database that contains (or will contain) personal data and indicate this on the job bag. A Data Classification Risk Assessment will be completed, this will ensure that proper procedures as defined in the ISMS will be adhered to throughout the production cycle.

Rapidity will keep some forms of information longer than others in line with Financial, Legal or Archival requirements.

**Data Retention and Disposal**
It is important that data retention and disposal arrangements are agreed at the outset of any project and the details defined on the job information area within Tharsterns.

In general terms no data will be stored after the completion of the project unless there is a specific request to do so.

All secure data will be downloaded from the SFTP server and held in a secure file, identified as such, which is not archived and will be deleted after use in line with the requirements of the client. Unless specifically requested, all data will form part of this process. The SFTP server is backed up on a daily basis and will be overwritten within 7 days.

If specifically requested the files can be data shredded to ensure that all disc space is wiped clean. Any data supplied on disc will be returned to the client after use. All procedures that are specific to a client will be recorded in the Quality Procedures under Special Procedures.

Data used for direct mailing will be kept until the project is complete. This data will be modified and kept up to date to ensure that it is current. Data that is bought in will be deleted when the project is finished. Records will be maintained of all deleted data files.

Any computer or piece of equipment that carries any data will have the hard drive destroyed before it is disposed of.

**Responsibilities of staff**
It is the responsibility of the Data Protection Officer to:

- Assess the understanding of the obligations of Rapidity staff under the Data Protection Act
- Be aware of our current compliance status
- Identify and monitor problem areas and risks and recommend solutions
- Promote clear and effective procedures and offer guidance to staff on data protection issues. This will include familiarisation with the regulations starting with the Induction process, training programmes/seminars, annual appraisals and intranet/internet resources.

It is **NOT** the responsibility of the Data Protection Officer to apply the provisions of the General Data Protection Regulations. This is the responsibility of the individual keepers and users of personal data. Therefore, staff are required to be aware of the provisions of the GDPR, keeping records up to date and accurate, and its impact on the work they undertake on behalf of Rapidity.

Any breach of the Data Protection Procedures, whether deliberate, or through negligence may lead to disciplinary action being taken or even a criminal prosecution.

**Data Security**
All staff are responsible for ensuring that:

Any personal data they hold, whether in electronic or paper format, is kept securely.

Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

**Subject Access Requests**
Rapidity is registered as a data processor any subject Access Requests received will be forwarded to the Data Collector (Client).