CONNEXUS
INFORMATION GOVERNANCE

GDPR AND INFORMATION RISK

What GDPR Means To You
Your Legal Obligations
Control Information Risk

www.connexus.consulting
08458 675 516

WHAT IS GDPR?

Keeping information about clients and staff confidential makes clear business sense but it is also required by law. **The EU General Data Protection Regulation (GDPR)** defines the ethical handling of personal data.

Replacing legislation written before the digital age, the regulation became EU law in 2016, enforceable from **25th May, 2018.** The new Data Protection Act 2017 is the UK's implemenation of GDPR. This booklet intends to introduce the key elements, without constituting legal advice, as further guidance continues to be prepared.

TERMINOLOGY

Personal Data is information relating to an identifiable living person, such as name, ID, location data, IP address, customer reference number or customer code. All personal data needs to be protected and kept secure. There is also a duty to destroy it when appropriate.

Sensitive Personal Data is a special category of personal data including data relating to racial / ethnic origin, trade union membership, physical / mental health, genetic data or biometric data. This information requires additional measures to protect it.

Data Subject: any individual to whom the personal data relates. Note that additional rules apply when data subjects are under sixteen years of age.

Data Controller: an organisation that determines the way in which personal data is processed. The controller must be able to demonstrate compliance with the

principles and ensure contracts with data processors comply with the GDPR. Each data controller must also pay a fee to the Information Commissioner's Office.

Data Processor: an organisation that processes personal data, but only in accordance with the instructions of the data controller. This can include subcontractors and agents. Processors must maintain records of personal data and processing activities and will have legal liability if responsible for a breach.

Processing: collecting, disclosing, storing, using or any other operation performed upon personal data. If you use personal data in any way you will be "processing" it.

PRINCIPLES

You must comply with six core principles. Article 5 of the GDPR requires that personal data shall be:

1. **Processed lawfully, fairly and in a transparent manner.** This means you must let individuals know how you will use their personal data.
2. **Collected for specified, explicit and legitimate purposes.** This means one of the following six available lawful bases for processing must be met and personal data collected for one purpose should not be used for another.
    - **Consent.** The data subject has explicitly consented to processing.
    - **Contractual necessity.** Processing is necessary in order to enter into or perform a contract with the data subject.
    - **Compliance with legal obligations.** The controller has a legal obligation to perform processing.
    - **Vital interests.** It is necessary to protect the vital interests of the data subject, essentially in life-or-death scenarios.
    - **Public interest.** Where necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.
    - **Legitimate interests.** The controller has a legitimate interest in processing data,

provided that such legitimate interest is not overridden by the rights or freedoms of the affected data subjects.

3. **Adequate, relevant and limited to what is necessary for the purposes for which it is processed.** This means you should only process the personal data that you actually need and no additional information which is not relevant.

4. **Accurate and kept up to date.** This means you have a duty to update any incorrect records.

5. **Kept for no longer than is necessary.** This means information should not be kept longer than is necessary and you should destroy personal data when you no longer have a reason to store it.

6. **Kept secure and confidential.** This means you must take steps to help ensure that data is not lost, stolen or unlawfully disclosed.

INDIVIDUAL RIGHTS

Data subjects have gained new rights and personal data must be processed in accordance with them, as below:

Right to be informed: You must provide 'fair processing information', typically through a privacy notice, advising how you will use personal data.

Right of access: Individuals can review personal data and verify the lawfulness of the processing.

Right to rectification: Individuals can demand their personal data is updated if it is inaccurate or incomplete.

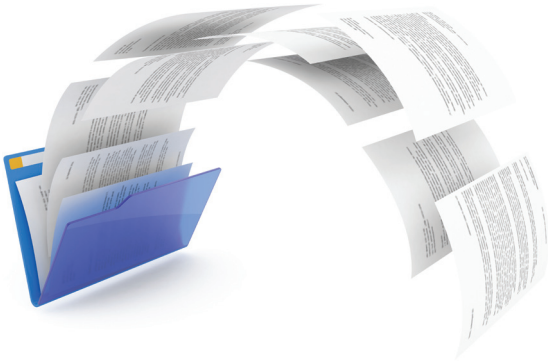
Right to be forgotten: Individuals can ask that their data is erased or removed if the organisation can no longer justify it being processed.

Right to restrict processing: Organisations will only be able to store, and cannot otherwise use personal data if:

- The accuracy of the data has been challenged and the data controller is verifying this.
- The individual has objected to the processing and the data controller is considering this.
- It is no longer lawful for the data controller to process the data but the individual has asked that the organisation restricts its processing rather than deletes the data.

- The organisation no longer requires the data but the individual requires it for the establishment or defence of a legal claim.

Right to data portability: Individuals can ask that their existing service provider transfers certain data to their new provider without delay.



Right to object: A controller must have a lawful basis for processing personal data. However, where that lawful basis is either "public interest" or "legitimate interests", those lawful bases are not absolute, and data subjects may have a right to object to such processing.

Rights in relation to automated decision making and profiling: In cases where decisions have legal (or other significant) effects, data subjects can refuse to be evaluated solely on the basis of automated processing.

ACCOUNTABILITY

You must be able to demonstrate that you have put suitable governance measures in place to protect personal data and minimise the risk of breaches. This is likely to be in the form of policies and procedures with accompanying user training. In some cases, there are additional requirements such as:

- Appoint a **Data Protection Officer** (DPO).
- **Privacy Impact Assessments:** Evaluation of the risks inherent in proposed data processing activities, which enables you to address and mitigate those risks before processing begins.
- **Privacy By Design:** a project approach to promote privacy and data protection compliance from the start.

SECURITY

Appropriate measures must be used to protect personal data against accidental loss, destruction or damage and unauthorised or unlawful processing.

INTERNATIONAL TRANSFERS

Personal data can only be transferred outside the European Economic Area if certain conditions are met.

PERSONAL DATA BREACHES

Any breaches must be reported within 72 hours of becoming aware of it, unless the breach is unlikely to result in any risk to individuals in question. If the breach is likely to result in high risk to the freedoms and rights of the individuals, then they must also be notified.

GDPR CHECKLIST

- [ ] Ensure key staff are aware of GDPR.
- [ ] Evaluate your current processing to help identify your obligations. What data do you collect, for whom and why? An Information Audit will help you record how and on what basis you process data.
- [ ] Review and update privacy notices.
- [ ] Review and update your data protection policy.
- [ ] Ensure you are obtaining suitable consent.
- [ ] Conduct impact assessments where necessary.
- [ ] Review and update your contracts with processors.
- [ ] Decide whether to appoint a DPO.
- [ ] Keep up to date. The Information Commissioner's Office (ICO) regulates and enforces data protection in the UK and is a good source of further information: www.ico.org.uk

INFORMATION RISK

PROTECTING REPUTATION AND ADVANTAGE

In addition to **personal data** which is subject to GDPR, your organisation stores **confidential** and **sensitive** information which could put your organisation at **significant financial, operational or reputational risk** if it ended up in the wrong hands. Your organisation may also be subject to **sector specific regulatory sanctions.** This content is *not* subject to GDPR, but has other potentially critical consequences. Information risk should be approached exactly as any other business risk, evaluating the risk of misuse against the level of risk the Board is prepared to accept.

INFORMATION GOVERNANCE

Information is your organisation's most valuable asset, so you must handle it responsibly. In addition to the GDPR obligations for personal data, adopting a broader Information Governance (IG) programme to manage and protect all digital information should be a part of day-to-day business.

INFORMATION GOVERNANCE:
"The activities and technologies
that organisations employ
to maximise the value of their information while
minimising associated risks and costs"

(Information Governance Initiative)

User filing of electronic data has removed the need for the filing clerk, who would meticulously ensure documents were properly managed and stored, enabling staff to locate the correct version of a record.

Whilst electronic filing has unquestionable benefits such as ease of access and searchable text, the lack of discipline in applying useful filenames and saving to logical locations has resulted in a common state of poor Information Governance.

High value business information which supports your ongoing success is frequently **buried or lost** within chaotic unmanaged repositories, often amidst records stored well beyond the approved retention schedule.

Giving relevant staff straightforward access to the right information is a cornerstone of business success. It is the organisations which embrace Information Governance that are giving themselves the best chance to excel in a competitive market.

BENEFITS OF EFFECTIVE IG

An enhanced Information Governance strategy will lead to significant business benefits, including:

- **Personal Data Protection**
  Ensure compliant management of files containing personal data.

- **Sensitive Data Protection**
  Ensure compliant management of files containing sensitive data.

- **Data Loss Prevention**
  Ensure protectively marked and sensitive data has not leaked into areas where it is at increased risk of Cyber Security breaches.

- **Increased User Productivity**
  Find the right information, which was previously buried in a mountain of data.

- **Enhanced User Collaboration**
  Shared information increases efficiency.

- **Retention Policy Implementation**
  Remove files when they become obsolete.

- **Storage Savings**
  Clarity on what to remove or quarantine and what costs this can save you.

- **Migration Efficiency**
  Migrate a lower volume of high value files to a new repository with consistent metadata.

10 STEPS TO BETTER IG

Having led, managed, planned and delivered hundreds of client projects of all sizes across the globe, these ten steps from our consultants may help you consider how to tackle your project:

01 Find Executive Sponsor

It is essential to gain support from your organisation's **executive management.** Encouraging the business to adopt your information governance processes is one of the key challenges you will need to overcome, and business users often struggle to justify contributing to IG projects without clear directives from those who are leading the business.

02 Build A Team

It may sound obvious, but we have seen many examples of ambassadors trying to engage single-handedly with the whole business. You will need to **build a supportive network of stakeholders** throughout the business. As a minimum, key representation from each business area should contribute department specific requirements and provide delegated access to experienced members of staff for relevant approvals. Involving IT is often critical, as gaining a rapid and deep understanding of information is usually only viable with software support.

03 Align Policy

A logical set of clear rules captured in a set of **policy documents are an essential foundation** for any information governance project. Policies such as Acceptable Use, Data Protection, Records Management and Dispoal are the essential link between legislated

corporate responsibilities and business user compliance. It is these clear guidelines which enable you to identify and deal with violations in order to ensure that policy is adhered to. A review of your existing policies, particularly when combined with the quantitative results from an Information Audit will help identify any weaknesses and areas for improvement.

04 Protect Sensitive Data

Your organisation will be incurring storage costs for information which also puts you at **financial, operational and reputational risk.** Identify and locate files which contain personal, confidential and sensitive data, review whether they need to be retained and if so, ensure they are suitably managed and protected, rather than left in open fileshares.

05 Encourage Sharing

This may initially sound contradictory to the previous advice to protect sensitive data, but despite collectively working for the same organisation with shared goals, we frequently see separate departments (and even individual users) working independently, with local siloes of documents which are only clearly visible to a very limited number of staff. As noted, there can be very good reasons for this, but we recommend a **first principle for business success is to share all information** between all users unless there's a good business case to restrict it. The most basic elements to encourage sharing and collaboration are to implement consistent file naming conventions and a simple logical accessible filing structure, so it is clear to other users where documents of any type should be stored, and to clearly identify them in that location. A common mistake made by many organisations is to implement a technology solution such as an Electronic Document and Records Management System, but **successful implementation of EDRMS requires a clear and practical Information Governance Strategy** as a solid foundation and framework for the management and use of information within the organisation. There are indeed clear benefits in moving content to a managed environment, but if done without considered preparation, the EDRMS merely becomes a new and more expensive place to store data, but one which has a more complex and daunting interface than the fileshares which business users are used to, hindering the adoption and success of the EDRMS.

06 Discourage Email

Email has become the primary method of business communication and software provides an easy mechanism for users to store records of business decisions. The issue with email is that such records are stored in independent and inconsistent structures which are only easily accessible to the recipient, clearly at odds with the previous advice to encourage sharing of information. An email system should only be used for transient communications, with all **business records exported to a collaborative environment,** where other users can benefit from access to that information. We have seen many businesses struggle with enforcing better email policy and management, but a very simple approach is to **progressively restrict mailbox size** (with accompanying communications, of course), which makes it impossible for users to maintain personal filing systems within their inbox.

07 Train Users

It sounds too simple to need to state, but we have seen many organisations attemping to implement steps to improve information governance centrally without considering that the whole business is affected. **Everyone will need guidance** on how to manage information, otherwise centralised efforts to cleanse and reorganise data will leave users confused, frustrated and fighting to restore to the original problematic state.

08 Communicate Progress

Do take the time to share your success stories, as **a good case study is surprisingly motivating** for more reticent heads of departments and staff. We have seen cases where some departments need to be reassured by seeing a plan working effectively before they consider adopting it, and other cases where simple departmental rivalry has led to a competitive approach to achieving the best results.

09 Build Momentum

A surprisingly common danger is that an extreme purist approach can lead to a target of unachievable perfection. **Start with a manageable and realistic set of deliverables,** and carefully consider trading off acceptable compromises to make more rapid progress.

Our advice is to start with smaller but achievable goals, so you learn from and build on your successes to gain momentum and support as you proceed.

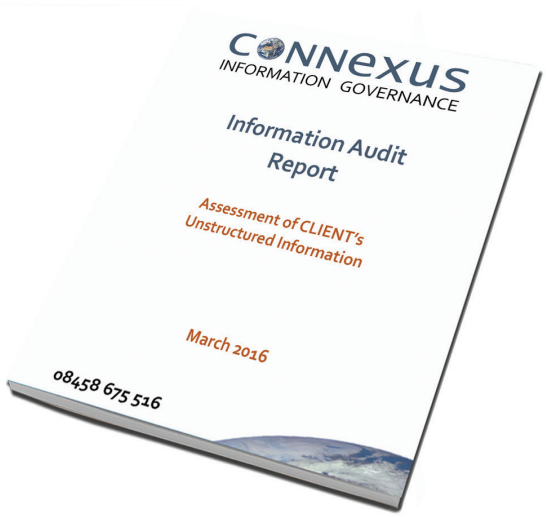
10 Develop Ongoing Plan

A common misconception is that information governance is a one-off activity. Whatever your organisation's situation, both business sense and legislation dictate you must address information governance as an ongoing part of day-to-day operations.

Connexus IG delivers an Information Audit to help you quantify and determine the true cost of each category of information, giving you a clear actionable policy and methodology.

With this information, we help you plan and deliver an ongoing course of action to take control. Once established, this becomes a repeatable and defensible process to take control of information risk.

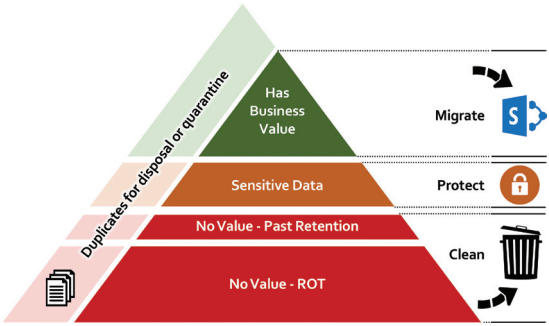
You will benefit from experienced world class consultants working on your project, coupled with market leading file analysis software for information governance, security and compliance.



INFORMATION AUDIT

It is challenging and time-consuming for users to effectively locate surplus and at risk information within your network.

You can pinpoint this data with an **Information Audit,** which identifies the issues and quantifies the growing scale of the problem.



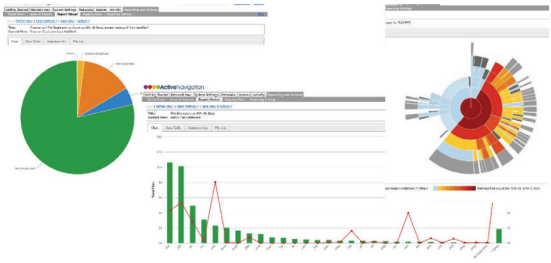
Information Audits are commonly offered as an accurate but intensive manual process by consultants or as fast but sometimes unpredictable software solutions. The ideal balance is achieved with a **cost-effective combined solution** which offers the speed of bespoke software coupled with the expertise of accomplished consultants.

An Information Audit should determine the **quality and health** of your digital landfill and **identify weaknesses,** concluding with a **plan of action** to improve your IG strategy. Connexus Information Governance offers a groundbreaking Information Audit at a **fixed fee** which can be completed in **less than a month.**

DELIVERABLES

The Connexus IG Information Audit can be tailored to your specific requirements, but a standard package will deliver the following:

- **Personal data subject to GDPR,** such as passports and utility bills
- **Sensitive financial data** such as credit card or bank account details
- Sensitive corporate information, such as **protectively marked data**
- **Custom record types,** such as trade secrets or child protection records



- **ROT** *(redundant, obsolete and trivial)* which has no value to your business and can be removed
- **Duplicates** which can be safely deleted
- Quantify **potential savings** through defensible cleansing
- Identify issues with **readiness for migration** to your chosen content repository
- **Collate, classify and tag** records for **migration**
- **Summarise results** with **detailed examples** from analysis
- Scale up to **hundreds of Terabytes of data**
- Offer recommendations for **enhancements to your existing policies**
- **Outline implementation plan** to improve Information Governance

We love to talk about Information Governance with people who are interested in hearing it! So, if you'd like to throw some of your questions and challenges at us, please get in touch with one of our helpful experts for some free advice.

CONNEXUS
INFORMATION GOVERNANCE

INFORMATION AUDIT
POLICY GUIDANCE
PROJECT PLANNING
ROT REMOVAL
SENSITIVE DATA REMEDIATION
METADATA TAGGING
CLASSIFICATION DESIGN
ECM MIGRATION

Information in a ***chaotic state?***
Redundant data ***expensive to store?***
Useful 'information' *hidden in 'data'?*
Users struggling to ***work collaboratively?***
Sensitive *&* ***confidential*** *files poorly managed?*
No-one can implement your ***retention policy?***
Data ***migration*** *frustrating and slow?*

An unrivalled combination of
world-class consulting *and*
revolutionary software *to improve the*
quality and health *of your digital landfill*

www.connexus.consulting
08458 675 516