Restore

Records Digital Datashred Relocation Technology

Data Protection Regulations

The impacts of the GDPR and DPA 2018: making sure you are compliant, with Restore Records Management

Foreword

The EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 represent the greatest change to UK data protection regulation in 20 years.

Charles Bligh,
Restore PLC
CEO

This change reflects the modern world, where the value of personal information to both organisations and individuals keeps increasing. The expectations of regulators, with powers to impose significant fines for serious breaches, should be viewed in the wider context of customers, service users and citizens – and their rights.

Of course, behind every piece of personal information is an individual. Enhanced individual rights in the GDPR emphasise this: the removal of fees for making access requests; the right to erasure where information no longer serves a purpose; the right to seek compensation should any failure lead to damage. The Information Commissioner's Office (ICO) notes that organisations that thrive under the new regulations are those that recognise that the legislation puts "the individual at the heart of the data protection law".

The ICO also highlights that the GDPR and DPA 2018 are about "placing the highest standards of data protection at the heart of how you do business" – and that's where Restore steps into the frame.

Restore's services are all about managing and handling data professionally, securely and strictly in line with current regulations. It's what we do, every day. We enable you, our customer, to serve your customers more consistently and efficiently while meeting the expectations of every individual who entrusts you with their personal information. And those fundamentals of trust and honesty are key values in the way we do business, too.

In this Data Protection Regulations brochure you will find information about our knowledgeable and approachable specialists. They can help you manage the ongoing impacts of the GDPR and DPA 2018 by conducting a full data protection assessment of your organisation. In another section, there is a 13-point examination of key areas for your consideration and in-depth research with the overarching theme of compliance – and how to achieve it throughout your organisation's systems and processes.

On subsequent pages, you will find that Restore is keen to equip all our customers with the right tools for the job. In the case of managing and, indeed, trying to eliminate the risk associated with handling confidential data correctly, we believe that our bespoke on-site file and asset tracking software – Dovetail – is fit for that purpose. Dovetail makes locating every trace of an individual's data history, whether on paper or digital, a smooth, efficient and effective operation. The software blends seamlessly with your management systems, as well as our own, and ensures an end-to-end electronic audit trail with ease of access, transparency and accountability built in, neatly meeting all regulatory requirements.

As with all the services we offer at Restore, underpinning our expertise, innovation and tools for data protection compliance is our desire to give you the best possible customer experience. I hope that you will find this Data Protection Regulations brochure is a step towards supporting you and your organisation in that goal.

Changes to Data Protection

The EU's General Data Protection Regulation (GDPR) was the result of four years' work by the EU to bring data protection legislation into line with new, unforeseen ways that data is now used.

Previously, the UK had relied on the Data Protection Act 1998, which was enacted following the 1995 EU Data Protection Directive, but the GDPR legislation supersedes this and is supported by the new Data Protection Act 2018. It has introduced much tougher fines and penalties for non-compliance and breaches and gives individuals more say over what companies can do with their data. It also makes data protection rules more or less identical throughout the EU.

When did the changes apply?

The GDPR has applied in all EU member states since 25 May 2018. Because GDPR is a regulation, not a directive, the UK did not need to draw up new legislation – instead, it applied automatically. However, the Data Protection Act 2018 reflects all the basic rights and articles of GDPR, with few variants, and is now UK law.

> The General Data Protection Regulation builds on the previous legislation, but provides more protections for consumers and more privacy considerations for organisations. It brings a more 21st century approach to the processing of personal data. And it puts an onus on businesses to change their entire ethos to data protection.
>
> **Elizabeth Denham, UK Information Commissioner**

13 areas the data protection regulations affect

01

IF YOUR BUSINESS IS NOT IN THE EU, YOU STILL HAVE TO COMPLY WITH THE REGULATION

Non-EU organisations that do business in the EU with EU residents' personal data need to comply with the Regulation

The **CONSEQUENCES** for failing to comply are the same.

02

THE DEFINITION OF PERSONAL DATA IS BROADER, BRINGING MORE DATA INTO THE REGULATED PERIMETER

Data privacy now encompasses more factors that can be used to identify an individual, such as their genetic, mental, economic, cultural or social identity. Companies should be taking measures to reduce the amount of personally identifiable information they store as a matter of course, and erasing it when it is no longer necessary.

03

CONSENT IS NECESSARY TO PROCESS CHILDREN'S DATA

Parental consent is required for the processing of personal data of children under the age of 16. EU member states may lower the age requiring parental consent to 13.

07

NEW DATA BREACH NOTIFICATION REQUIREMENTS

Data controllers must report data breaches to their data protection authority unless it is unlikely to present a risk to the rights and freedoms of the data subjects in question.

08

THE RIGHT TO ERASURE

Or the 'right to be forgotten' – a phrase made famous by the European Court of Justice ruling against Google Spain in 2014. The data DPA 2018 provides clear guidelines about the circumstances under which the right can be exercised.

04

THE RULES FOR OBTAINING VALID CONSENT HAVE CHANGED

Your consent document should be laid out in simple terms. Also, silence or inactivity does not constitute consent. Clear and affirmative consent to the processing of private data must be provided.

05

A DATA PROTECTION OFFICER (DPO) IS MANDATORY FOR CERTAIN COMPANIES

A DPO should be in place in companies where the core activities of the controller or the processor involve regular and systematic monitoring of data subjects on a large scale or where the entity conducts large-scale processing of special categories of personal data.

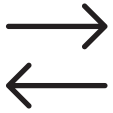
06

PRIVACY RISK IMPACT ASSESSMENTS ARE MANDATORY

In order to analyse and minimise the risks to their data subjects, data controllers must adopt a risk-based approach and are required to conduct privacy impact assessments where privacy breach risks are high.

09

THE INTERNATIONAL TRANSFER OF DATA



The regulation also applies to processors, so organisations should be aware of the risk of transferring data to countries that are not part of the EU.

10

DATA PROCESSOR RESPONSIBILITIES

Under the GDPR and DPA 2018, data processors have direct legal obligations and responsibilities, which means they can be held liable for data breaches.

11

DATA PORTABILITY

Data portability enables the user to request a copy of personal data in a format usable by them and electronically transmissible to another processing system. This aims to make users independent from any one company's services.

12

PRIVACY BY DESIGN

The DPA 2018 requires that systems and processes comply with the principles of data protection by design and by default. Privacy in a service or product should be taken into account right from the inception of the product concept.

13

ONE-STOP SHOP

Businesses only have to deal with a single supervisory authority in each EU member state. In the UK, this is currently the Information Commissioner's Office (ICO).

> The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability

Information Commissioner's Office, 2017

Does data protection apply to you?

The Data Protection Act (DPA) 2018 applies to **'controllers' and 'processors'**. The definitions are broadly the same as under the Data Protection Act 1998, the controller says how and why personal data is processed, and the processor acts on the controller's behalf. If you were subject to the previous law, you will be subject to DPA 2018.

The **Data Controller** is the 'individual or business' that designates the required activity for a piece of data, both on the purpose of the data activity and how that piece of data is processed. In the event of a data breach, only the data controller would be liable for compliance and not the processor. All responsibilities are transferred to a data processor via a 'data processing agreement'.

If you are a controller, the obligation is on you to ensure your contracts with processors comply with the DPA 2018.

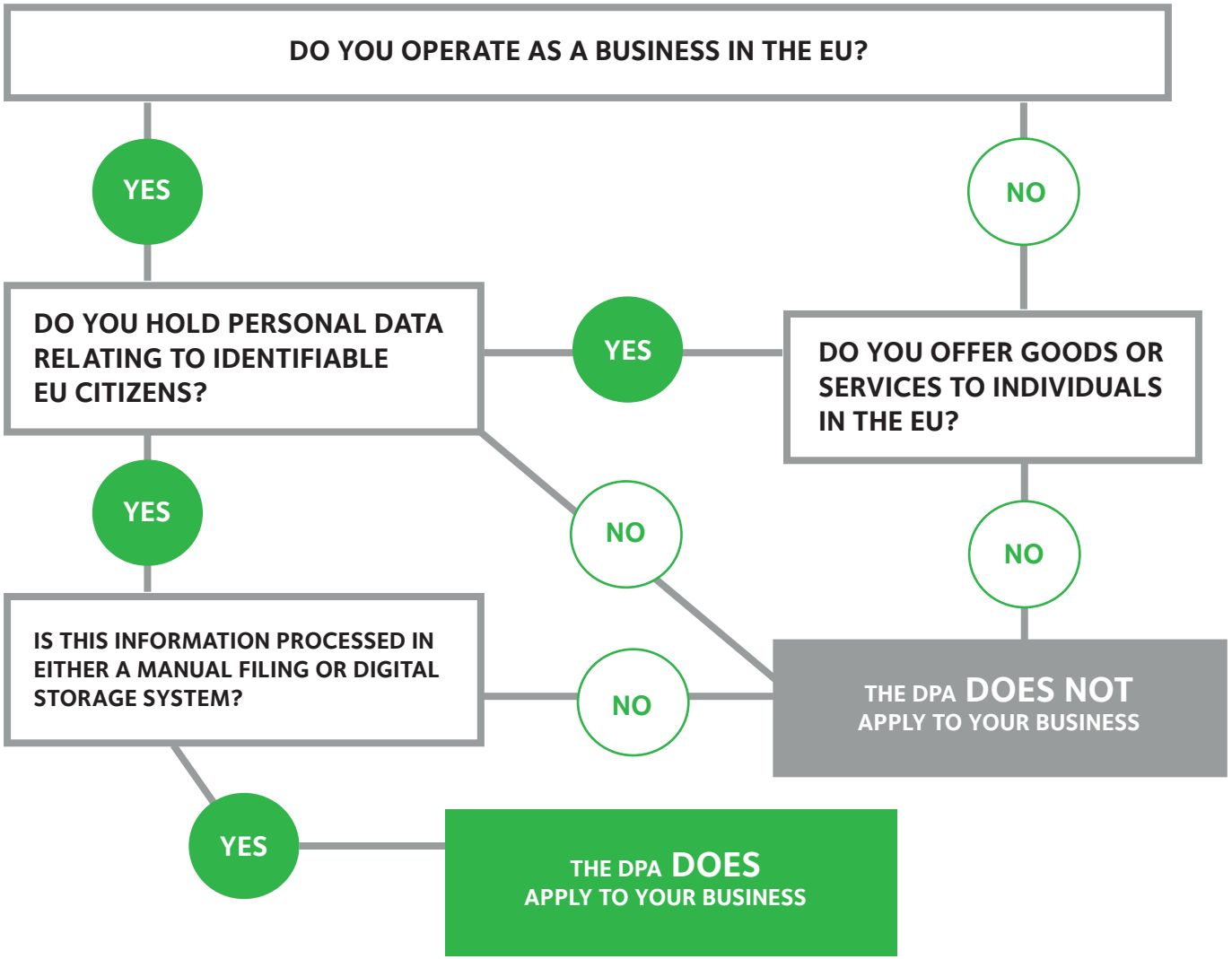
The **Data Processor** is an 'individual or business entity' that processes information on behalf of a data controller via a data processing agreement. Only personal data shared on behalf of the controller may be processed, these are the mandatory terms as set out in the DPA 2018.

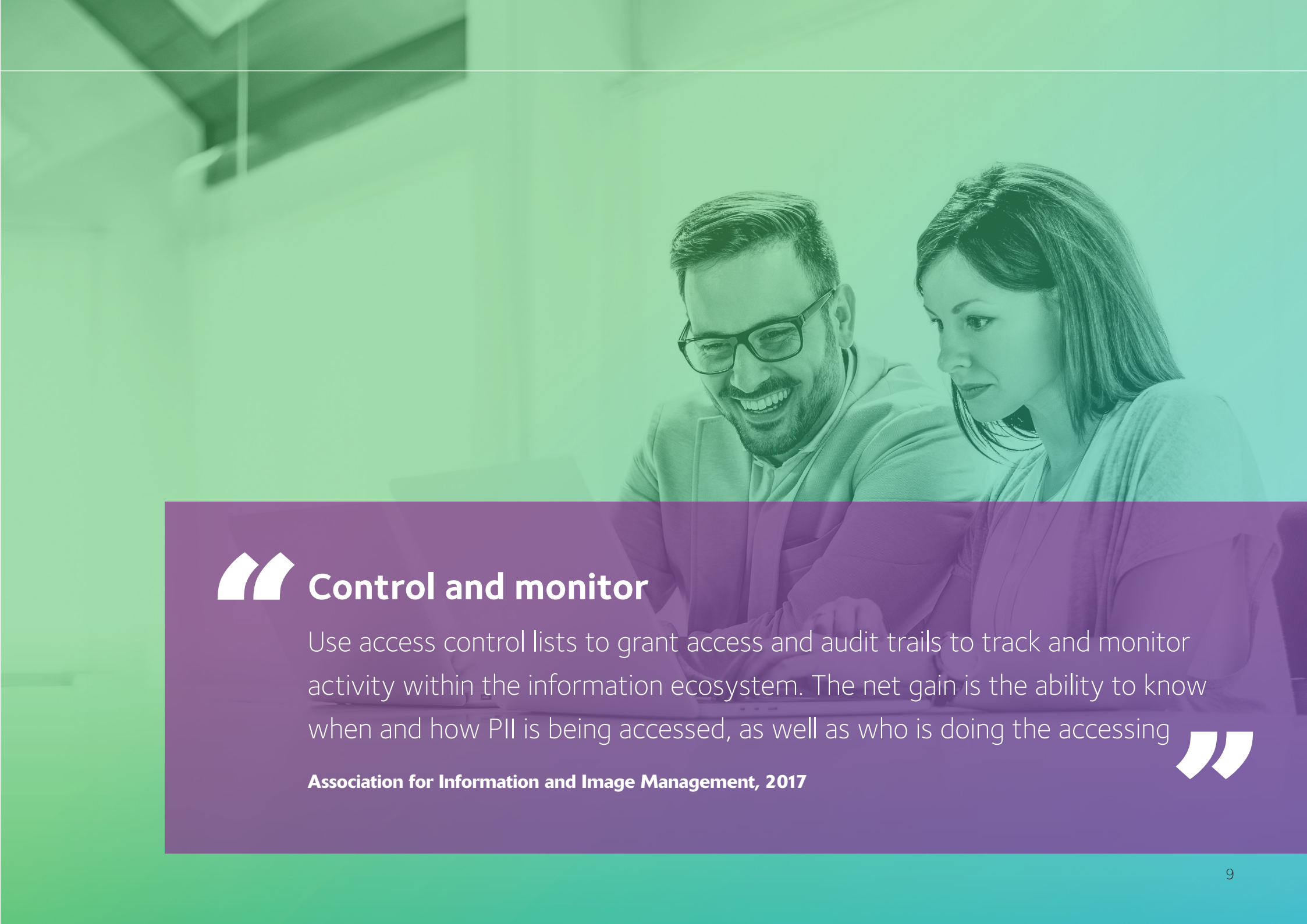
If you are a processor, the DPA 2018 sets specific legal obligations on you. For example, you are required to maintain records of personal data and processing activities. You have significantly more legal liability if you are responsible for a breach. These obligations for processors are an additional requirement under the DPA 2018.

Primary considerations

- The DPA 2018 applies to 'personal data' relating to identifiable EU citizens, including names, ID number, location data, contact data and online identity. The DPA 2018's definition makes it clear that information such as an online identifier – an IP address, for example – is personal data too.
- The DPA 2018 applies to organisations that keep data such as employment records, financial information, educational records, medical records, marketing or customer lists, social security numbers. It cuts across all vertical sectors.
- The DPA 2018 applies to both automated personal data and to manual filing systems where personal data are accessible. This could include chronologically ordered sets of manual records containing personal data.
- The DPA 2018 also refers to sensitive personal data as 'special categories' of personal data. The particular categories include genetic data and biometric data where processed to uniquely identify an individual.
- The DPA 2018 applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The DPA 2018 does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.
- There are some subtle differences between the GDPR and the DPA 2018 in areas such as the processing of criminal data, automated decision making and processing, privacy versus freedom of expression and data subject rights. In the case of the latter, for instance, the GDPR ensures that all data subjects have rights in relation to the processing of their personal data. The DPA allows these rights to be ignored if compliance with these rights would seriously impact an organisation's ability to carry out their functions when processing data for scientific, historical, statistical and archiving purposes. For full details, please speak to one of our data protection specialists on 0808 278 3679.

Follow our four-question flowchart to see if the DPA applies to your company





Control and monitor

Use access control lists to grant access and audit trails to track and monitor activity within the information ecosystem. The net gain is the ability to know when and how PII is being accessed, as well as who is doing the accessing

Association for Information and Image Management, 2017

We're here to help

In the ever-evolving regulatory landscape, paper records represent a significant compliance risk. To help companies ensure their paper records don't fall foul of the Regulation, we have a team of experienced business consultants and digital specialists on hand to help you fully understand the impact of the GDPR, and the DPA 2018, on your organisation. We will help you identify gaps and formulate a roadmap for compliance that does not just remove uncertainty, but enables you to deliver better outcomes, build trust with your customers and significantly reduce any associated risks.

Find the information you need

The right to erasure, also known as 'the right to be forgotten', is the broad principle that enables an individual to request the deletion or removal of personal data where there is no legal reason for its continued processing. Before you can de-identify or delete information, you will need to be able to find it.

While it may be easy to search for and remove digital data from a record or database, hard copies can be far harder to locate quickly. Even where an individual does not request erasure of their information, personal information cannot be held in a form that permits identification for longer than is necessary for the purposes for which it is processed. This makes the management of personal information, from creation through to secure destruction, more critical than ever.

We can help you with:

- **Digital imaging and data extraction programs that will streamline your organisation's ability to store, access and manage documents in an electronic format**
- **A precise filing and identification system for all paper records, with tags, barcodes and meta data marked on individual files and storage boxes, with clearly defined access rights and accountabilities**
- **Secure destruction services for paper documents, hard drives and electronic media, issuing a certificate of destruction after every shred**

Multiple copies of Personal Identifiable Information (PII)

Many organisations already have clearly defined processes for information management, from the creation of data through to secure destruction. However, paper documents can slip through the cracks of even the strictest information storage policies, simply by being copied or printed and left lying around, carelessly disposed of, or removed from a secure building during an office move.

We can help you with:

- **Ensuring data is kept no longer than necessary by applying automatic retention policies for both physical data in storage such as documents and media tapes, as well as digital data**
- **Automated solutions such as digital mailrooms to capture all documents as soon as they enter your organisation, mitigating the risk of generating multiple paper versions of the same information**
- **Secure transportation of your IT and data when organising an office move**
- **IT disposal, CESG-approved destruction technologies to carry out degaussing, software wiping and physical destruction of all media types, in compliance with the WEEE directive**

Right of access

Under the GDPR and DPA 2018, 'right of access' has an additional set of obligations for data controllers. This means that a data subject has the right to request confirmation from the controller as to whether his/her data is being processed. The controller will have to allow access to that personal data and to provide the data subject with a copy of the data upon request.

We can help you with:

- **Document scanning services, coupled with indexing for back-scanning, operational-scanning and scan-on-demand services, facilitating robust search capability**
- **Quality check, index, cleanse and securely host your documents in the Cloud, enabling accessibility from anywhere in the EU, and across any device**
- **Audit, indexing and storage of PII data in fully secure archiving facilities that are purpose built to store and protect documents**

How to mitigate the risk of reputational damage, penalties from the ICO and compensation claims

The potential financial penalties for the most serious breaches of the GDPR have significantly increased: maximum fines of £17.4million or 4% of worldwide annual turnover (whichever is the higher) could be issued for, among other things, retaining identifiable personal data for longer than is necessary and failing to comply with individual rights of access and requests for erasure.

Even if the ICO, the UK's supervisory authority set up to uphold information rights, does not take regulatory action, individuals can now seek compensation should they suffer material or non-material damage as a result of an infringement of the GDPR. For example, if an organisation is unable to locate the entirety of an individual's information and either disclose it (in response to a request) or delete it (following a request for erasure), it could constitute a claim. If the failure led to an individual's reputation being damaged, significant economic or social disadvantage, deprives them of their rights and freedoms or prevents them from exercising control over their personal information, this too could constitute a claim.

The reputational damage to an organisation of being unable to demonstrate adequate management of personal information can be greater, and longer lasting, than any one penalty or series of compensation claims.

We can help you with:

- **Indexing the exact data you hold, spanning both physical documents and digital documents**
- **Delivering powerful search facilities to make responding to DSAR (Data Subject Access Requests) quick and easy**
- **Monitoring and access control for confidential documents, with full audit trails**
- **Applying different security levels to documents, records and folders**
- **Managing both electronic and paper documents to minimise risk of breach and loss**
- **Automating workflows to reduce manual intervention**
- **Encoding of destruction dates, online systems, eventual data destruction**
- **Our own on-site file and asset tracking software – Dovetail – for files, computer tapes, hospital X-rays, and so on. (Turn to page 14 for more details about Dovetail.)**

Individuals' rights

You should check your procedures to ensure they cover all the rights people have, including how you would delete personal data or provide data electronically and in a commonly used format

Information Commissioner's Office, 2017

Introducing complete control, with Dovetail

How to be data protection compliant by creating integrated end-to-end data processing systems

Dovetail

Dovetail is our bespoke on-site file and asset tracking software that we adapt to your business so that you can track every piece of information from desk to desk, office to shelf, for the whole of its lifecycle wherever you keep it. Dovetail interfaces with your existing management systems and blends seamlessly with ours.

Use Dovetail to track:

- **Files**
- **Mortgage deeds**
- **Leases**
- **X-rays**
- **Patient records**
- **Computer tapes**
- **Whatever you need to control**

> Dovetail takes your data security responsibilities as seriously as you do. Use Dovetail to keep sensitive, personal information private and shared by the few, not the many. You can nominate specific individuals, small teams or whole departments for access. Even when interfacing with off-site data management software, that customer data stays private too and auditable by your nominated network – closing gaps for risk and ensuring your and your customers' peace of mind.

How Dovetail helps you achieve data protection compliance

1. It can help solve GDPR and DPA 2018-related challenges by integrating multiple data sources, making process status instantly visible and making content stored across different locations a non-issue
2. It is a single management hub, which ensures the correct levels of access, privacy and security for processing subjects' data and increases productivity by up to 25%!
3. Dovetail is a tool for Data protection Officers (DPOs), who are responsible for monitoring data processing, assessing and reporting on risk, advising senior management and notifying data subjects and the ICO of breaches
4. It helps reduce archive size by up to 20% through superior auditing of retention periods and disposal deadlines
5. Dovetail helps your data processor in accurate file tracking and auditing of data and asset movements because it can 'dovetail' seamlessly with their own systems
6. Our software isolates specific data with ease and can help certify an audit trail right through to destruction. So you can confidently satisfy data subjects who wish 'to be forgotten'

Not only that...

...Dovetail enables an improved user experience, better customer experiences, business agility and more productive teams!

Records Digital Datashred Relocation Technology

Restore can help you build a practical plan that will not only help you manage data protection compliance but also future-proof your organisation.

Take the first step towards your data protection assessment.
Contact us to find out more about our range of services.

03300 376 323

restore.co.uk

Restore Records Management

22 MILLION ITEMS IN STORAGE

Store and manage all your business-critical documents, back-up tapes and heritage items.

Restore Digital

238 MILLION IMAGES SCANNED

Transform your organisation through digitisation and automated workflows.

Restore Datashred

100 THOUSAND TONNES SHREDDED

Scale, efficiency, value and unrivalled customer service from the UK's leading document destruction provider.

Restore Harrow Green Moving Professionals

250+ THOUSAND PEOPLE MOVED EACH YEAR

Market leading business relocation made to measure.

Restore Technology

500+ THOUSAND DESKTOPS MOVED

The complete set of services for your IT assets.

bsi. ISO 9001 Quality Management
bsi. ISO 14001 Environmental Management
bsi. ISO/IEC 27001 Information Security Management
bsi. Partners in Excellence Programme
NAID
The Institute of Customer Service
CIWM
CPNI Centre for the Protection of National Infrastructure