ISO SYSTEMS UK

Intelligent Management Systems

Practical • Simple • Flexible

# Conducting a Data Flow Mapping Exercise Under the GDPR

December 2018

Practical • Simple • Flexible

# INTRODUCTION

The EU General Data Protection Regulation (GDPR) superseded the EU member state implementations of the 1995 Data Protection Directive (DPD) on 25 May 2018. In response to this, the UK's new Data Protection Act (DPA) 2018 replaced the DPA 1998. All UK organisations that handle personal data must comply with both the Regulation and the new DPA.

The GDPR extends the rights of individuals, and requires organisations to implement appropriate technical measures, as well as clear policies, procedures and other organisational measures to protect personal data. The penalties for failing to comply with the Regulation are potentially severe. Administrative fines can be up to €20 million or 4% of annual global turnover in the preceding financial year – whichever is greater. The Regulation says that these penalties will be "effective, proportionate and dissuasive".

# DATA FLOW MAPPING

Data flow mapping is a key step in ensuring compliance with the GDPR. Organisations often process much more data than they realise, and data flow maps help them to identify the data they hold and where it is moving.

It is important to walk through the information lifecycle to identify unforeseen or unintended uses of data. Doing so can eliminate unnecessary data transfers and ensures that employees are aware of the practical implications of data usage. Tracking the interaction points between the parties involved – both internal and external – ensures that all uses of the data can be identified. A data flow map can also be used to make sure data subjects are aware of how their data is used.

The future uses of data also need to be properly thought out, even if an organisation has no immediate plans. By predicting how data will be used in months or years to come, organisations can make sure they have appropriate resources and security measures in place and give data subjects advanced notice.

# THE KEY ELEMENTS

Intelligent Management Systems

A data flow map should identify:

- Data items
- Formats
- Transfer methods
- Locations

These elements need to be established because each can introduce different risks to the data. The data items are the details of the information itself, i.e. a person's name, email, address, etc.

The format of the data refers to the methods by which the data is collected, stored, processed and released. Is it obtained as a hard copy (paper records), via a form on a website, harvested from emails, or some other method? The organisation then needs to look at how the data is being transferred – is it by post, telephone, secured connection or social media, and is the transfer internal or external?

The organisation will also need to look into the location of the data and where it is stored. This could be in an office, in the Cloud, with a third party, and so on.

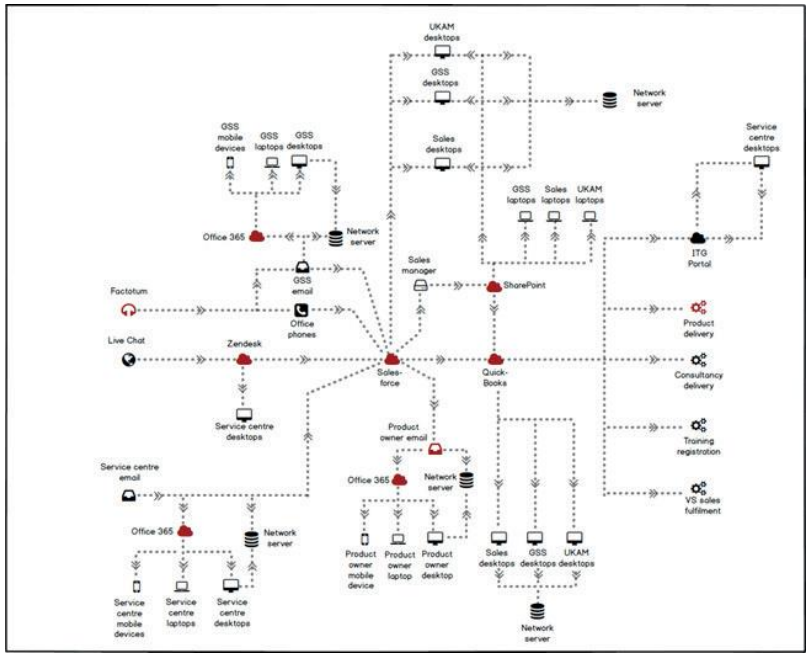



*Figure 1: Detailed data flow map*

# UNDERSTANDING THE DATA

One of the first challenges is to determine what personal data is being collected. There are many different types of personal data, such as names, ID numbers, passport numbers, IP addresses, usernames, medical records and biometric data. Any such information will be subject to the GDPR if it relates to an identifiable, living person.

You must also identify the source of the data and the circumstances under which you are collecting it. What kinds of technical and organisational safeguards are in place to protect the rights and freedoms of the data subjects? The GDPR is, after all, about protecting individuals, not the entity that collects the data. An organisation needs to understand its legal and regulatory obligations, and ensure it meets those obligations.

# MAPPING TECHNIQUES

There are several ways organisations can gather information about their processing operations.

Information can be collected by inspecting existing documents, running workshops, conducting questionnaires or observing business activities. If your organisation does not already have a documented workflow describing how personal data is collected and processed, it can be worthwhile to send out a team to investigate.

An organisation can also work with team members to discuss what happens at each stage of the data collection process, clarifying where the data goes and who sees it. Tools and templates, including data flow mapping applications, could help with these discussions and ultimately map data.

# WORKFLOW INPUTS & OUTPUTS

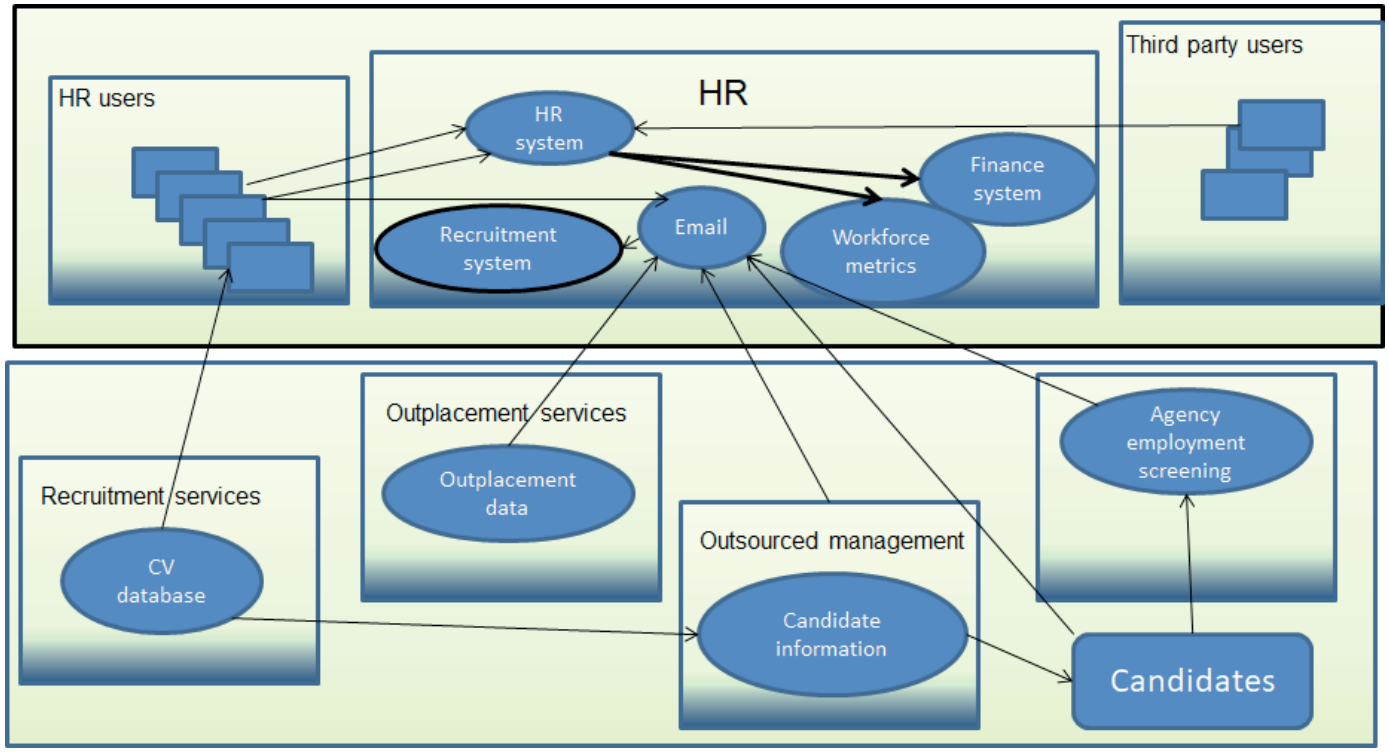
A workflow has data coming in one end and going out the other, with some process happening to the data in between. In many cases, the output of a process or a workflow provides the input for another.

Understanding workflows requires you to understand the personal data and the form it has been collected in. You need to look at how the data was captured, who is accountable for it, where it is located and who has access to it. You then need to establish if the information has been disclosed/shared with anyone, and if the workflow interfaces with or transfers information to any other processes.

The previous page shows an example of a detailed data flow. Its complexity enables the organisation to identify what it needs to do to manage its data.

This example looks only at the processing of personal data within a general sales team, by contrast, below is an example of a less structured data flow, looking at how CVs might be processed in a recruitment campaign or as part of an organisation's recruitment process.

This data flow shows the different ways in which the data is coming in, the number of people who will use the data and where the data is going. An organisation needs to be able to track each of these movements in order to put the appropriate checks in place, such as controls managing transfers to third parties involved in the process. Ensuring these measures are appropriate to privacy and other related risks is an essential part of GDPR compliance.



# THE PRACTICAL STEPS

Gathering the necessary information to populate your data flow maps is critical. A data flow audit can be used to gather this information and construct data flow maps.

## Step 1 – Document your processing

The first step is to document the scope and purposes of processing. You cannot work out the impact on the rights and freedoms of natural persons unless you know what data you have and where it is flowing. If you are not sure how you handle personal data, you cannot provide assurances that data protection is fundamental to how you operate.

As you run your data flow audits, you should also build a personal data inventory. If you are not aware of all the data your organisation possesses, you cannot reliably accommodate data subject access requests, in contravention of the GDPR.

When building a personal data inventory, you need to establish the data items, data subject and the lawful basis for processing.

## Step 2 – Mapping and inventory

The next step is to enter this information into a data map. This will provide a visual depiction of the data you hold, how it moves through the organisation and where it is processed.

## Step 3 – Include related assets

Step three is to add the supporting assets used to process personal data. These include any location where data is stored or used, such as an app or a report file, as well as processes that involve personal data, such as secure destruction.

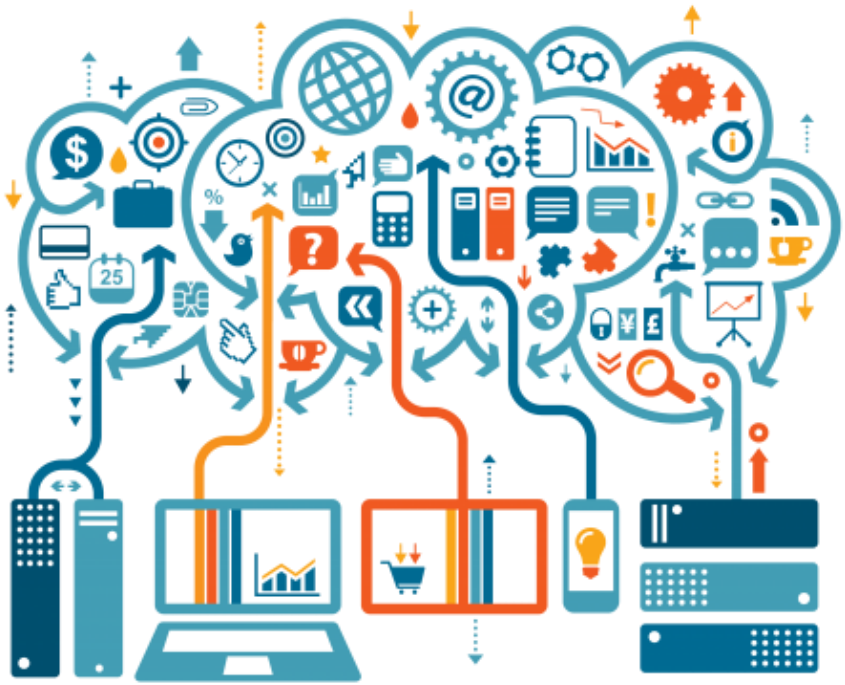
Assets form part of the control environment – for instance, if personal data is managed by a device that uses an unpatched operating system, a range of vulnerabilities are introduced that must be dealt with as part of the organisation's risk management activities.

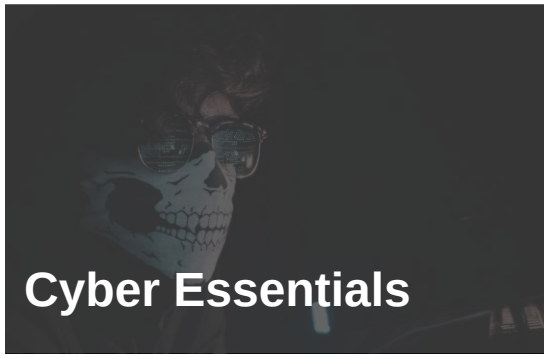
## Step 4 – Map data transfers

Step four is to add data transfers to the map to show the flow of data between assets, so that you can make sure there are no intermediate steps. It also enables you to consider security in the data flows, both when the data is in transit and when it is at rest.

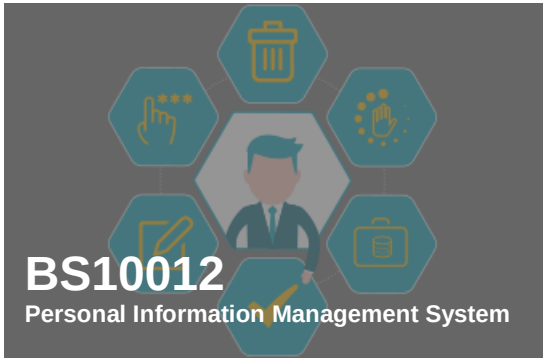
## Step 5 – Review

The final step is to review the process to ensure there is nothing you have missed. The outputs of the data mapping will help your organisation meet its obligations under the GDPR, so it is essential that the results are thorough. In particular, this will help your organisation develop a record of processing activities (Article 30 of the GDPR) and identify activities that may need to be reviewed with a data protection impact assessment (DPIA).








ISO SYSTEMS UK

Intelligent Management Systems

Practical • Simple • Flexible

Find out more at: www.isosystems.org.uk/isoconsultancy

# Contact Us


E: billynaisbett@isosystems.org
M: 07791 425 011

## Get in Touch

It is the policy of ISO Systems UK to provide our clients with the most competitive, flexible, responsive and qualified service possible.

But we know that no person can be an expert in all elements of every available standard, tool, technique and methodology.

If we don't specialise, we won't advertise, but if our client wants it, we will use a close team of specialist professionals to assist where it is not our standard project type to fulfil the exact requirements and the needs of our clients.

Please feel free to contact us with any questions that you may have, we will be pleased to assist - professional, friendly advice does not have to cost!


E: scott@isosystems.org
M: 07813 858 310