FORUM of PRIVATE BUSINESS

For our members, not for profit

A Guide to the GDPR

Prepare for ***The General Data Protection Regulation (GDPR)*** that is replacing the ***Data Protection Act 1998*** from **25th May 2018**.

GDPR APR2018

fpb.org

Notes

A guide to the new General Data Protection Regulations (GDPR)

Contents

Notes

Introduction to the GDPR

The new EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation for 20 years and will apply from 25th May 2018.

The new regulations are vast and how they are to be implemented will be bespoke to each business.

The Forum is here to help make sure your business is prepared. We recommend that you read this guide through carefully, follow the steps and use the useful links at the end of the guide for more information.

Due to the complexity of the GDPR, you may find it difficult leaving your preparation until the last minute. Alternatively, you may feel more reassured speaking to a professional.

The aim of the GDPR

New data protection laws are being introduced with the aim of protecting the personal data of individuals living in the EU and to harmonise data privacy laws across Europe. The GDPR will also facilitate the secure, free-flow of data between member states.

The GDPR has been driven by the need to tackle data inconsistencies throughout Europe while bringing the law up to date with the rapid developments in technology.

What is the GDPR?

The GDPR is a modernisation of data protection laws drawn up in 1995, before mass internet adoption, email and google search.

As a consequence, the current data protection rules are no longer fit for purpose. Even though the key principles of data privacy still hold true, there have been many new changes that will significantly impact the way a business is run and how information is captured and shared.

The new *General Data Protection Regulations (GDPR)* will come into force on 25th May 2018. Businesses now need to ensure that processes are put in place and changes are made to their current data protection procedures in order to meet and adhere to the new regulations.

It is also important to note that countries outside the EU, dealing with individuals within the EU, must also comply with the new regulations when dealing with personal data. For example, a company in America who deals with personal data from individuals in Spain must comply with the GDPR.

Although the UK is leaving the EU, the UK Government has confirmed that this will not affect the commencement of the GDPR and the EU regulations will likely form part of UK law after Brexit.

The GDPR details the principles of the new data privacy rules, but how you meet and comply with the regulations has to be determined by you.

Each company should have individual compliance strategies designed to meet the regulations, depending on the nature of your business and how you process personal data. This guide will take you through, step-by-step, the actions you will need to take to ensure your business is compliant with the GDPR.

Why is the GDPR so important?

Forty six percent of UK businesses experienced a breach of their cyber security or were victim to a cyber-attack in the twelve months between April 2016 and April 2017.

Cyber security is a huge issue and its importance is growing due to the increasing risk of cyber-attacks that small business and organisations face every day, not only in the UK but on a global scale.

It is now essential that businesses across Europe protect the data rights of their citizens. The GDPR will succeed in doing this by putting the control back in the hands of the people by introducing strict fines to ensure that all EU businesses take data protection seriously.

The impact of Brexit

The scope of the GDPR applies to any business within the EU or holds data of EU citizens. When Brexit takes place, the UK will still be a member of the EU until 2019 and, as such, the penalties for non-compliance of the GDPR will still need to be enforced.

Even when we are out of the EU, the ICO has announced that it will be taking the EU GDPR into UK legislation, so the UK will have its own version of the GDPR.

What information does the GDPR apply to?

The GDPR applies to all personal data and therefore has a huge impact on businesses trading in the UK.

What is personal data?

Personal data is any data that can be used to identify an individual, either directly or when combined with other information.

Personal data includes, but is not limited to, details such as name, address, email address, mobile number, bank account details, credit card number, driver/passport number, online name, genetic or biometric data, and metadata including IP address, mobile IMEI numbers and SIM card IDs.

Do you have a process for amending/deleting personal data?

This is a good time to check your procedures. If an individual calls your business and asks for their personal data to be deleted, for example, would your internal systems and procedures be able to cope with this? If not, you will need to consider whether revisions need to be made to your internal procedures to ensure business compliance by 25th May.

Who is responsible for implementing the GDPR in a business?

Decision makers and key people within the business need to be aware that the data law is changing as they will be expected to put into place comprehensive but proportionate governance measures in order to comply with the GDPR.

These measures are required in order to protect personal data and to minimise the risk of breaches.

You may find that your business already has good governance measures in place. However, it is still important that you can demonstrate the necessary compliance across areas such as staff training, internal audits and reviews of HR policies, to name but a few.

Data controller and data processors

It is essential for businesses involved in the processing of personal data to be able to determine whether they are acting as a data controller or a data processor. It is the responsibility of both to comply with the GDPR as fines can be applied to both parties.

The data controller determines the purposes and means by which personal data is processed and is responsible for demonstrating compliance with the principles and requirements of the GDPR.

A checklist for data controllers has been created by the Forum with small organisations in mind. The set-by-step approach helps to guide businesses and data controllers through the detail proving essential reading for both our members and non-members. The checklist, can be found on **page 13**. Please refer to the full range of checklists on **page 12**.

The data processor carries out processing of personal data on behalf of the Controller. This could involve the obtaining, recording, holding, altering and retrieval of data.

The data controller must ensure that they only use data processors who can guarantee they implement measures and procedures required to meet the GDPR.

A checklist for data processors has been created by the Forum with small organisations in mind. The set-by-step approach helps to guide businesses and data processors through the detail proving essential reading for both our members and non-members. The checklist, can be found on **page 45**. Please refer to the full range of checklists on **page 12**.

Why do you need to comply with GDPR?

Penalties for non-compliance can be eye-watering with fines up to €20 million or 4% of business worldwide turnover, whichever is higher.

This is a huge increase from the old data protection laws where maximum fines reached £500,000. The rules apply to both controllers and processors. However, the Information Commissioner's Office (ICO), which is the Data Protection Authority in the UK, have said they will use the penalty powers 'proportionately and judiciously'.

Whatever size of your business, it's important to dedicate the necessary time to preparing for the GDPR.

How to make your business compliant

Whatever your business, there are a number of important areas to consider when complying with the GDPR and any appropriate action needs to be taken before 25th May 2018.

Evidence of compliance

Accountability and good governance are central to effective and compliant data processing and are essential to the process of complying with the GDPR.

Not only should a business aim for full compliance, it should also now be able to evidence full compliance.

The GDPR sets out various ways an organisation can demonstrate and document compliance, including:

- Reviewing and implementing data protection processes.
- Putting into effect internal organisational measures, such as company policies and procedures.
- Where appropriate, appointing a data protection officer to oversee processing within the organisation.
- Undertaking a data protection impact assessment (DPIA), where appropriate.

Privacy by default

Privacy by default ensures that only as much personal data is collected, used and kept for each task as is needed.

In particular, businesses will need to ensure personal data is not automatically made available to third parties without the individual's intervention.

Privacy by design

Privacy by design means the implementation of data protection from the onset of designing systems, rather than an afterthought.

Businesses must ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle.

- Building new IT systems for storing or accessing personal data.
- Developing legislation, policy or strategies that have privacy implications.
- Embarking on a data sharing initiative; or
- Using data for new purposes.

Organisations should be integrating core privacy considerations into existing project management and risk management methodologies and policies.

The GDPR checklist for data sharing and subject access from the ICO is relevant for businesses who want to assess their data sharing policies and agreements. The checklist can be completed on **page 65**. Please refer to the full range of checklists on **page 12**.

Storing data

Personal data cannot be stored outside of the EU and data cannot go back and forth beyond EU boundaries.

Businesses must consider their CRM systems, email distribution etc. to ensure the data is not going beyond EU boundaries. You must also provide accessible and detailed records of how data is used, where and by whom. The data collected must have restricted access and permissions.

The GDPR checklist for direct marketing from the ICO is relevant for companies who are involved in the marketing to individuals using telephone, email, text and post. Further details, including the checklist, can be completed on **page 99**. Please refer to the full range of checklists on **page 12**.

Consent

Individuals must actively give consent to how their data is used. Implied consent is not acceptable and therefore considered a breach of data.

Consent must be specific and state the exact purpose why the data is being collected and used. Companies can no longer use long illegible terms and conditions full of legal jargon. Consent must be easily understood and accessible using clear and plain language. You must be able to demonstrate that consent has been given freely and it must also be as easy for an individual to withdraw their consent as it is to give it.

Breach notification

You must ensure you have processes in place to detect, report and investigate a data breach.

Any data breach that is likely to risk an individual's rights and freedoms, must be notified to the supervising authority – Information Commissioner Office (ICO) - and any data subjects of any data breach within seventy-two hours of becoming aware of the breach. If it is not likely to risk an individual's rights and freedoms, it does not need to be reported. If you are unsure, speak to the ICO for advice.

The ICO do not expect a full comprehensive report at the initial data breach notification, but they do need to know the potential scope and cause of the breach and how you plan to deal and address the problem.

Failure to report a breach could result in a fine, along with a fine for the breach itself.

Individuals' rights

It is important to check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. The GDPR includes the following rights for individuals:

Right to erasure (forgotten)

Individuals can ask for their personal data you store to be completely erased.

It can be erased if the data is no longer relevant to its original purpose, or the data subject withdraws their consent. If you have disclosed the personal data in question to third parties, you must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

As a business you must put processes in place to carry out any requests for erasure quickly and thoroughly and at no cost to the individual.

Right to be informed

At the point of data collection, you must clearly explain to the individual how their personal data is intended to be used.

You can no longer just use simple opt-in and out boxes, the intention of the data must be easily accessible and explained in clear and plain language and provided free of charge. If challenged and found non-compliant this is considered a data breach

Right to access

Under the new regulations, individuals have the right to obtain information from a company as to how their personal data is being processed, where and for what purpose.

It must also be provided within one month of receipt of their request and in electronic format. You can extend the time to respond by two months if it is a complex request.

Right to data portability

Individuals can request their data to be moved, copied or transferred from one supplier of service to another.

As a business you must put processes in place to carry out any requests for this quickly and thoroughly. The data must be in a readable format so other organisations can extract and use the data. You may be required to send the data directly to another organisation, if this is possible. This must be provided free of charge.

Right to rectification

If personal data is incorrect, individuals have the right to have this rectified.

If you have sent the original data to a third party, you must also inform them of the changes to be made. You must action the request within a month, or two months if it is a complex change.

Right to restrict processing

There are a few instances when you have to restrict the processing of personal data.

You are permitted to store the data but not process any of the data.

You must restrict processing in the following instances:

- When an individual contends the accuracy of the data.
- When an individual has objected to their data being processed.
- Restriction can be requested instead of erasure from the individual.
- You no longer need the data but the individual needs their data to be stored for a future legal claim.

If you have given the personal data to a third party, you must inform them a restriction has been put in place.

Right to object

Individuals have the right to object to their personal data being processed.

Individuals can achieve this in the following ways:

- Processing based on legitimate interests or the performance of a task in the public interest/ exercise of official authority (including profiling).
- If you process data in relation to the above and the individual objects, you must stop processing unless you can demonstrate legitimate grounds for the processing or the processing is for the establishment, exercise and defence of legal claims.
- Direct marketing. If an individual objects to their data being used for direct mail, you must stop using their data immediately and you cannot dispute their objection.

- Processing for purposes of scientific/historical research and statistics.
- An individual can object to their personal data being used for research and statistics but they must have grounds to their objection, 'relating to his or her particular situation'.

If the processing of the data is necessary for the performance of a public task you do not have to comply with the objection.

Rights to related automated decision making and profiling

Under the GDPR, data processing may be characterised as "profiling" when it involves automated processing of personal data; and using that personal data to evaluate certain personal aspects relating to a natural person.

An automated decision is a decision which is made following processing of personal data solely by automatic means, where no humans are involved in the decision-making process. The rights of an individual in relation to an automated decision only arise where the automated decision can have a significant impact on the individual (e.g. where the decision relates to the individual's job performance or credit worthiness). These rights exist so that no potentially serious decisions regarding an individual is taken without human involvement.

The new regulations will provide a protection for individuals where a potentially damaging decision could be made about them. Individuals will have the right to not be subjected to an automated decision and are able to obtain a decision through human intervention.

Children

Children are less aware of the risks involved with a data breach and so need particular protection when handling and processing their personal data.

Business systems and processes need to take this in to account and age appropriate safeguards put in place.

Next steps

- **Designate or appoint a Data Protection Officer (DPO)**. You may be required to formally designate a DPO if your business carries out large scale processing of data or a public authority.
- **Carry out a risk assessment on your business**. Document all current processes and data flows and analyse any potential areas of weakness or vulnerability.
- **Complete the relevant GDPR checklist(s) from the ICO**. Complete the checklist (s) at the back of this guide dependant on your role and business to assess where you are compliant and to uncover any gaps.
- **Carry out a gap analysis**. Identify the level of compliance which then allows you to detect areas which need improving.
- **Check all of your business relationships** with service providers, data providers and contractors and find out if they are compliant under the GDPR.
- **Review all privacy notices** and ensure they comply with the new regulation requirements.
- **Amend any documents** that allude to data processing.
- **Update all data protection policies.**

- **Carry out a data protection impact assessment (PIA)** for high risk projects.
- **Maintain detailed records of processing operations and activities** and consider if you have the required data processing agreements in place.

How the Forum can help your business with the GDPR?

The Forum has a team of membership advisors on hand to answer your calls about the GDPR and to discuss with you what you need to do to ensure your business is compliant by 25th May 2018.

We have also worked with the ICO to create easy-to-use GDPR checklists that can be completed relevant to role and business. These checklists will identify where you are complaint and help you to uncover the areas that need focus before the 25th May 2018.

GDPR checklists

There are six different checklists available for you to complete, dependant on your role and business type. It is advisable to allow yourself the time to complete these thoroughly by the GDPR deadline. The checklists are listed below and can all be found later on in the guide.

Page 13 - GDPR checklist for data controllers

Page 45 - GDPR checklist for data processors

Page 65 - GDPR checklist for data sharing and subject access

Page 79 - GDPR checklist for information security

Page 99 - GDPR checklist for direct marketing

Page 107 - GDPR checklist for records management

Page 127 - GDPR checklists for CCTV

Useful links

EU GDPR
www.eugdpr.org

ICO
www.ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/

Data controllers
www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-controllers/

Self-assessment toolkit for data controllers, **page 13**

Data processors
www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-processors/

Self-assessment toolkit for data processors, **page 45**

GDPR and children
www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/

GDPR checklist for data controllers

Notes

GDPR checklist for data controllers

This GDPR checklist has been created by the ICO (Information Commissioners Office) to help prepare businesses for the new data protection laws due to come in to force on 25th May 2018. We believe this to be a useful tool for our members and non-members and for all small to medium sized organisations from the private, public and third sectors.

Effective information handling makes good business sense. You will enhance your business's reputation, increase customer and employee confidence and, by making sure personal information is accurate, relevant and safe, save both time and money.

Do you process personal data as a data controller or a data processor?

Before you undertake the GDPR checklist you should first determine whether your role is as a data controller or as a data processor.

The definition of the two terms are:

Data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which any personal data is, or is to be, processed.

Data processor is responsible for processing personal data on behalf of a controller. If you are the data processor, the GDPR places specific legal obligations on you. For example, you will be required to maintain records of personal data and processing activities and you will have legal liability if you are responsible for a breach.

Checklist for data controllers

The process of completing the checklist will enable a business to assess their compliance with data protection law and will help you to ascertain what you need to do to make sure all personal data is safe and secure.

The checklist is broken down in to four steps. Due to its length and detail, it is advisable to set aside plenty of time to complete all four steps effectively. To complete the checklist online, please visit **www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-controllers/**

On completion, a short report will be created suggesting practical actions you can take to ensure GDPR compliance. It will also provide links to additional guidance that will help ensure your business meets the new data protection laws.

Checklist for data processors

This section of the guide contains the checklist for a data controller only. However, if your role is as a data processor, we suggest you complete the data processor checklist that can be found on **page 45** of this guide.

www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-controllers/

In some instances, an organisation will process personal information as both a controller and a processor. When this is the case, the ICO would advise that both checklists for a data controller and a data processor are completed.

Step 1 of 4: Lawfulness, fairness and transparency

1.1 Information you hold

Your business has conducted an information audit to map data flows.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should organise an information audit across your business or within particular business areas. One person with in-depth knowledge of your working practices may be able to do this. This will identify the data that you process and how it flows into, through and out of your business.

Remember, an information flow can include a transfer of information from one location to another. For example, the information may stay within your business yet a transfer takes place because the department or other office is located elsewhere (off site).

Having audited your information, you should then be able to identify any risks.

Suggested actions

You should:

- Organise an information audit across your business or within particular business areas to identify the data that you process and how it flows into, through and out of your business.
- Ensure this is conducted by someone with in-depth knowledge of your working practices.
- Identify and document any risks you have found, for example in a risk register.

Guidance

Find out what information you have, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/find-out-what-information-you-have/**

Identify information assets, National Archives **www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf**

Your business has documented what personal data you hold, where it came from, who you share it with and what you do with it.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Once you have completed your information audit, you should document your findings, for example, in an information asset register. Doing this will help you to comply with the GDPR's accountability principle, which requires your business to be able to show how you comply with the GDPR principles. For example, by having effective procedures and guidance for staff.

If you have **less than 250 employees** then you must keep records of any processing activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

If you have **over 250 employees**, you must record the following information:

- Name and details of your business (and where applicable, of other controllers, your representative and data protection officer).
- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Where applicable, details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- A general description of technical and organisational security measures.
- You may be required to make these records available to the ICO on request.

Suggested actions

You should:

- Maintain records of processing activities detailing what personal data you hold, where it came from, who you share it with and what you do with it. This will vary depending on the size of your business;
- Consider using an information asset register to do this; and
- Ensure you have procedures to guide staff on how to manage information you hold.

Guidance

Identify information assets, National Archive **www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf**

Information Asset Register template, National Archive **www.nationalarchives.gov.uk/documents/information-management/iar_template.xls**

1.2 Lawful bases for processing personal data

Your business has identified your lawful bases for processing and documented them.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You need to identify lawful bases before you can process personal data and special categories of data.

Your lawful bases for processing have an effect on individual's rights. For example, if you rely on someone's consent to process their data, they will have a stronger right to have their data deleted. It is important that you let individuals know how you intend to process their personal data and what your lawful bases are for doing so, for example in your privacy notice(s).

Suggested actions

You should:

- Look at the various types of data processing you carry out.
- Identify your lawful bases for carrying it out.
- Document it, for example in your privacy notice(s).

Guidance

Guide to the GDPR - Lawful basis for processing, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/**

1.3 Consent

Your business has reviewed how you ask for and record consent.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The GDPR sets a high standard for consent but remember you don't always need consent. You should also assess whether another lawful bases is more appropriate.

Consent means offering people genuine choice and control over how you use their data. You can build trust and enhance your business by using consent properly.

The GDPR builds on the DPA standard of consent in several areas and contains much more detail:

- Keep your consent requests separate from other terms and conditions.
- Consent requires a positive opt-in. Use unticked opt-in boxes or similar active opt-in methods.

- Avoid making consent a precondition of service.
- Be specific and granular. Allow individuals to consent separately to different types of processing wherever appropriate.
- Name your business and any specific third party organisations who will rely on this consent.
- Keep records of what an individual has consented to, including what you told them, and when and how they consented.
- Tell individuals they can withdraw consent at any time and how to do this.

Suggested actions

You should:

- Check that consent is the most appropriate lawful bases for processing.
- Make the request for consent prominent and separate from your terms and conditions.
- Ask individuals to positively opt-in.
- Use unticked opt-in boxes or similar active opt-in methods.
- Use clear, plain language that is easy to understand.
- Specify why you want the data and what you're going to do with it.
- Give granular options to allow individuals to consent separately to different types of processing wherever appropriate.
- Name your business and any specific third party organisations who will rely on this consent.
- Tell individuals they can withdraw consent at any time and how to do this.
- Ensure that individuals can refuse to consent without detriment.
- Don't make consent a precondition of service.

Your business has systems to record and manage ongoing consent.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Your obligations don't end when you first get consent. You should continue to review consent as part of your ongoing relationship with individuals, not a one-off compliance box to tick and file away.

Keep consent under review, and refresh it if anything changes. You should have a system or process to capture these reviews and record any changes.

If your current consent doesn't meet the GDPR's high standards or is poorly documented, you will need to seek fresh GDPR-compliant consent, identify a different lawful basis for your processing (and ensure continued processing is fair), or stop the processing.

Suggested actions

You should:

- Keep a record of when and how you got consent from the individual.
- Keep a record of exactly what they are told at the time.
- Regularly review consent to check that the relationship, processing and the purposes have not changed.
- Have processes to refresh consent at appropriate intervals, including any parental consent.
- Consider using privacy dashboards or other preference management tools as a matter of good practice.
- Make it easy for individuals to withdraw their consent at any time and publicise how to do so.
- Act on withdrawals of consent as soon as you can.
- Don't penalise individuals who wish to withdraw consent.
- If current consent don't meet the GDPR's high standards or is poorly documented, your business will need to;
    - Seek fresh GDPR-compliant consent.
    - Identify a different lawful bases for your processing (and ensure continued processing is fair).
    - Stop the processing.

1.4 Consent to process children's personal data for online services

If your business relies on consent to offer online services directly to children, you have systems in place to manage it.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

If you offer online services to children and you rely upon consent, only a child aged 13 or over will be able to provide their own consent.

You will therefore need to make reasonable efforts to verify that anyone giving their own consent is old enough to do so.

For children under 13 you will need to get consent from whoever holds parental responsibility for the child - unless the online services you offer are for prevention or counselling.

You must make reasonable efforts (using available technology) to verify that the person giving such consent does, in fact, hold parental responsibility for the child.

Suggested actions

You should:

- Have a process in place to verify the age of an individual (to determine if they are 13 years old or under) to confirm if they are old enough to provide consent themselves.
- If not relying on consent, identify the most appropriate lawful bases for the processing.
- Document your lawful bases for processing.
- Obtain parent or guardian's consent or authority if you want to rely on consent as the lawful bases for your processing.

Guidance

Guide to the GDPR - Applications - Children, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/**

1.5 Registration

Your business is currently registered with the Information Commissioner's Office.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Until May 2018, you are still required to register with the ICO (unless an exemption applies).

After May 2018 you need to pay the ICO a data protection fee.

Suggested actions

You should continue to register with the ICO if you annual registration is due before May 2018.

Guidance

ICO fee and registration changes next year, ICO blog **www.iconewsblog.org.uk/2017/10/05/ico-fee-and-registration-changes-next-year/**

Step 2 of 4: Individuals' rights

2.1 Right to be informed including privacy notices

Your business has provided privacy notices to individuals.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Individuals need to know that their data is collected, why it is processed and who it is shared with.

You should publish this information in your privacy notice on your website and within any forms or letters you send to individuals.

The information must be:

- Concise, transparent, intelligible and easily accessible.
- Written in clear and plain language, particularly if addressed to a child.
- Free of charge.

The information you supply is determined by whether or not you obtained the personal data directly from the individual or from a third party. See the link below for further information.

Suggested actions

Your privacy notice should:

- Let individuals know who you are, why you are processing their data and who you share it with.
- Be concise and to the point.
- Be easy to understand.
- Be clearly signposted and easy to access.
- Be written in clear and plain language, particularly if addressed to a child.
- Free of charge.
- Include different information depending on whether you obtained the data directly from the individual or not.
- Be reviewed regularly to make sure it remains accurate and up to date.

Guidance

Guide to the GDPR - Right to be informed, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/**

2.2 Communicate the processing of children's personal data

If your business offers online services directly to children, you communicate privacy information in a way that a child will understand.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You must provide children with the same fair processing information as you give adults. It will be good practice to also explain the risks involved in the processing and the safeguards you have put in place.

Any information directed at the child should be concise, clear, and written in plain language. It should be age appropriate and presented in a way that appeals to a young audience.

If you are relying upon parental consent as your lawful bases for processing it will be good practice to provide separate privacy notices aimed at both the child and the responsible adult.

If you provide online services and children younger than your target age range and they are likely to try and access it then it will be good practice to explain any age limit to them in language they will understand.

Suggested actions

Your privacy notice should:

- Be concise, transparent, intelligible and easily accessible.
- Be written in clear and plain language that can be understood by a child (age appropriate).
- Explain the risks involved in the processing and the safeguards you have put in place.
- Be free of charge.
- Be reviewed regularly to make sure it remains accurate and up to date.
- If you are relying upon parental consent as your lawful bases for processing it will be good practice to provide separate privacy notices aimed at both the child and the responsible adult.

2.3 Right of access

Your business has a process to recognise and respond to individuals' requests to access their personal data.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Individuals have the right to obtain:

- Confirmation that their data is being processed.
- Access to their personal data; and
- Other supplementary information – this largely corresponds to the information that you should provide in a privacy notice.

You should provide a copy of the information free of charge. However, you can charge a 'reasonable fee' when a request:

- Is manifestly unfounded or excessive, particularly if it is repetitive, unless you refuse to respond; or
- Is for further copies of the same information (that's previously been provided). This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

You will have less time to comply with a subject access request under the GDPR. Information must be provided without delay and at least within one calendar month of receipt. You can extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation).

A calendar month ends on the corresponding date of the next month (e.g. 2 January to 2 February), unless that date does not exist in which case it is the last day of the next month (e.g. 31 January to 28 February).

This means that the legal deadline will vary from 28 days to 31 days depending on the month. For practical purposes if a consistent number of days is required (e.g. for a computer system), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

You must verify the identity of the person making the request, using "reasonable means".

If the request is made electronically, you should provide the information in a commonly used electronic format.

Suggested actions

You should:

- Ensure a process is in place to allow you to recognise and respond to any subject access requests within the timescales.
- Include subject access procedures within your data protection policy.
- Provide awareness training to all staff and specialist training to individuals who deal with any requests.
- Consider if you can provide remote access to a secure self-service system to provide the information directly to an individual in response to a request (this will not be appropriate for all organisations, but there are some sectors where this may work well).

Guidance

Guide to the GDPR - Right of access, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/**

2.4 Right to rectification and data quality

Your business has processes to ensure that the personal data you hold remains accurate and up to date.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Individuals have the right to have personal data rectified if it is inaccurate or incomplete.

You should respond to a request without delay and at least within one month of receipt.

You can extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation). If you have disclosed the personal data to a data processor (third party) you must inform them of the rectification where possible.

You should regularly review the information you process or store to identify when you need to do things like correct inaccurate records. Records management policies, with rules for creating and keeping records (including emails) can help.

Conducting regular data quality reviews of systems and manual records you hold will help to ensure the information continues to be adequate for the purposes of processing (for which it was collected).

You should also ensure that there are regular data quality checks completed to provide assurances on the accuracy of the data being inputted by staff.

If you identify any data accuracy issues, communicate lessons learned to staff through ongoing awareness campaigns and internal training.

Suggested actions

You should:

- Implement procedures to allow individuals to challenge the accuracy of the information you hold about them and have it corrected if necessary.
- Have procedures to inform any data processors (third parties) you have disclosed the information about the rectification where possible.
- Create records management policies, with rules for creating and keeping records (including emails).
- Conduct regular data quality reviews of systems and manual records you hold to ensure the information continues to be adequate for the purposes of processing (for which it was collected).
- Regularly review information to identify when you need to correct inaccurate records, remove irrelevant ones and update out-of-date ones; and
- Promote and feedback any data quality trends to staff through ongoing awareness campaigns and internal training.

Guidance

- Guide to the GDPR - Right to rectification, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/**

2.5 Right to erasure including retention and disposal

Your business has a process to securely dispose of personal data that is no longer required or where an individual has asked you to erase it.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Individuals have the right to have personal data rectified if it is inaccurate or incomplete.

Individuals have the right to be forgotten and can request the erasure of personal data when:

- It is no longer necessary in relation to the purpose for which it was originally collected/processed.
- The individual withdraws consent.
- The individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- It was unlawfully processed (i.e. otherwise in breach of the GDPR).
- It has to be erased in order to comply with a legal obligation; or
- It is processed in relation to the offer of information society services to a child.

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- Archiving purposes in the public interest, scientific research historical research or statistical purposes.
- The exercise or defence of legal claims.

A written retention policy or schedule will remind you when to dispose of various categories of data, and help you plan for its secure disposal.

You should regularly review your retention schedule to make sure it continues to meet business and statutory requirements and any amendments should be agreed with managers and incorporated into the new schedule.

You should designate responsibility for retention and disposal to an appropriate person.

Suggested actions

You should:

- Have procedures in place which allow individuals to request the deletion or erasure of their information your business holds about them where there is no compelling reason for its continued processing.
- Have procedures to inform any data processors (third parties) you have shared the information with about the request for erasure.
- Have procedures to delete information from any back up systems.
- Implement a written retention policy or schedule to remind you when to dispose of various categories of data, and help you plan for its secure disposal.
- Regularly review the retention schedule to make sure it continues to meet business and statutory requirements.
- Assign responsibility for retention and disposal to an appropriate person.
- Have appropriate methods of destruction in place to prevent disclosure of personal data prior to, during and after disposal.
- If you use third parties to dispose of personal data ensure the contract includes the requirement for them to have appropriate security measures and the facility to allow you to undertake an audit.

Guidance

Disposal of Records, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/**

2.6 Right to restrict processing

Your business has procedures to respond to an individual's request to restrict the processing of their personal data.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Individuals have a right to block or restrict the processing of personal data.

When processing is restricted, you are permitted to store the personal data, but not further process it.

You can retain just enough information about the individual to ensure that the restriction is respected in the future.

You will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your businesses legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to be retained to allow them to establish, exercise or defend a legal claim.

You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

You must inform individuals when you decide to lift a restriction on processing.

Suggested actions

You should:

- Review your procedures to determine where you may be required to restrict the processing of personal data.
- Implement a process that will enable individuals to submit a request to you.
- Have a process to act on an individual's request to block or restrict the processing of their personal data.
- Have procedures to inform any data processors (third parties) you have shared the information with, if possible.
- Inform individuals when you decide to lift a restriction on processing.

Guidance

Guide to the GDPR - Right to restrict processing, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/**

2.7 Right of data portability

Your business has processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

They can receive personal data or move, copy or transfer that data from one business to another in a safe and secure way, without hindrance.

The right to data portability only applies:

- To personal data an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.
- Where the processing is carried out by automated means. Information must be provided without delay and at least within one month of receipt.

You can extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation).

You must provide the personal data in a structured, commonly used and machine readable format. Examples of appropriate formats include CSV and XML files.

You must provide the information free of charge.

If the individual requests it, you may be required to transmit the data directly to another business where this is technically feasible.

Suggested actions

You should:

- Implement a process that will enable individuals to submit a request to you.
- Have a process to allow you to recognise and respond to any individual requests in line with your legal obligations and statutory timescales.
- Provide the personal data in a structured, commonly used and machine readable format.
- Ensure that the medium in which the data is provided has appropriate technical measures in place to protect the data it contains.
- Ensure that the medium in which the data is provided allows individuals to move, copy or transfer that data easily from one organisation to another without hindrance.

Guidance

Guide to the GDPR - Right to data portability, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/**

2.8 Right to object

Your business has procedures to handle an individual's objection to the processing of their personal data.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/ exercise of official authority (including profiling).
- Processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on "grounds relating to his or her particular situation".

However for processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority or for purposes of scientific/historical research and statistics you must stop processing the personal data unless:

- You can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The processing is for the establishment, exercise or defence of legal claims.

Individuals also have the right to object to any processing undertaken for the purposes of direct marketing (including profiling). You must stop processing for direct marketing as soon as you receive an objection. There are no exemptions or grounds to refuse.

You must inform individuals of their right to object "at the point of first communication" and clearly lay this out in your privacy notice.

Suggested actions

You should:

- Review your processes and privacy notice(s) to ensure they inform individuals of their right to object "at the point of first communication". This information should be displayed or given clearly and separately from any other information.
- Implement a process that will enable individuals to submit an objection request (this could include an online option).
- Have processes in place to investigate an individual's objection to the processing of their personal data within the legitimate grounds outlined within the GDPR.
- Provide training or raise awareness amongst your staff to ensure they are able to recognise and respond (or know where to refer the request to) to an objection raised by an individual.

2.9 Rights related to automated decision making including profiling

Your business has identified whether any of your processing operations constitute automated decision making and have procedures in place to deal with the requirements.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Individuals have the right not to be subject to a decision when:

- It is based on automated processing.
- It produces a legal effect or similarly significant effect on the individual.

The right does not apply if the decision:

- Is necessary for entering into or performance of a contract between you and the individual.
- Is authorised by law (e.g. for the purposes of fraud or tax evasion prevention).
- Is based on the individual's explicit consent, and your business has put in place suitable measures to safeguard the individual's rights, freedoms and legitimate interests.

If suitable measures to safeguard the rights of data subjects are required, these must include at least:

- Obtain human intervention.
- Express their point of view.
- Obtain and explanation of the decision and challenge it.

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- Performance at work.
- Economic situation.
- Health.
- Personal preferences.
- Reliability.
- Behaviour.
- Location.
- Movements.

If the decision involves the processing of special categories of personal data then the exceptions available to justify the processing are more limited.

Processing can only take place if:

- You have the explicit consent of the individual and suitable measures to safeguard their rights, freedoms and legitimate interests are in place.
- The processing is necessary for reasons of substantial public interest, proportionate to the aim pursued.

You should exercise particular caution if using automated decision making in relation to a child.

Suggested actions

You should:

- Identify whether any of your processing operations constitute automated decision making.
- Ensure that, within any automated processing or decision making you undertake, individuals are able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.
- Implement appropriate safeguards when processing personal data for profiling purposes.
- Ensure that any automated decisions do not contravene the restrictions outlined within Article 9 (2) of the GDPR.

Guidance

Guide to the GDPR - Rights related to automated decision making including profiling, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/**

Step 3 of 4: Accountability and governance

3.1 Accountability

Your business has provided privacy notices to individuals.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The GDPR requires you to show how you comply with the principles.

A policy will help you address data protection in a consistent manner and demonstrate accountability under the GDPR. This can be a standalone policy statement or part of a general staff policy.

The policy should clearly set out your approach to data protection together with responsibilities for implementing the policy and monitoring compliance.

The policy should be approved by management, published and communicated to all staff. You should also review and update the policy at planned intervals or when required to ensure it remains relevant.

Suggested actions

You should have a standalone policy statement or general staff policy that:

- Sets out your business's approach to data protection together with responsibilities for implementing the policy and monitoring compliance.
- Aligns with and covers the measures within this checklist as a minimum.
- Is approved by management, published and communicated to all staff.
- Is reviewed and updated at planned intervals or when required to ensure it remains relevant.

Guidance

Policy examples and templates are widely available online.

Your business monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Documenting policies alone is often not enough to provide assurances that staff are adhering to the processes they cover. You should ensure that you have a process to monitor compliance to data protection and security policies.

Measures that are detailed within the policies should be regularly tested to provide assurances as to their continued effectiveness.

Responsibility for monitoring compliance with the policy should be independent of the persons implementing the policy, to allow the monitoring to be unbiased. Results of compliance testing should then be reported on a regular basis to senior management.

Suggested actions

You should:

- Establish a process to monitor compliance to the policies.
- Regularly test the measures that are detailed within the policies to provide assurances that they continue to be effective.
- Ensure that responsibility for monitoring compliance with the policies is independent of the persons implementing the policy, to allow the monitoring to be unbiased.
- Report any results to senior management.

Your business provides data protection awareness training for all staff.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should brief all staff handling personal data on their data protection responsibilities. It is good practice to provide awareness training on or shortly after appointment with updates at regular intervals or when required.

Specialist training for staff with specific duties, such as, information security and database management and marketing, should also be considered.

The regular communication of key messages is equally important to help reinforce training and maintain awareness (for example intranet articles, circulars, team briefings and posters).

Suggested actions

You should:

- Provide induction training on or shortly after an appointment.
- Update all staff at regular intervals or when required (for example, intranet articles, circulars, team briefings and posters).
- Provide specialist training for staff with specific duties, such as marketing, information security and database management.

Guidance

Think privacy toolkit, ICO website **www.ico.org.uk/for-organisations/resources-and-support/posters-stickers-and-e-learning/**

Training checklist for small to medium sized organisations, ICO website **www.ico.org.uk/media/for-organisations/documents/1606/training-checklist.pdf**

3.2 Data processor contracts

Your business has a written contract with any data processors you use.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Whenever you use a processor you need to have a written contract in place.

The contract is important so that both parties understand their responsibilities and liabilities. The GDPR sets out what needs to be included in the contract.

In the future, standard contractual clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the moment no standard clauses have been drafted.

You are liable for your processor's compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor that adheres to an approved code of conduct or certification scheme may help you to satisfy this requirement – though again, no such schemes are currently available.

Processors must only act on your documented instructions. They will, however, have some direct responsibilities under the GDPR and may be subject to sanctions if they don't comply.

Suggested actions

You should:

- Ensure that whenever your business uses a processor (a third party who processes personal data on your behalf) there is a written contract in place.
- Check both new and existing contracts now include certain specific terms, as a minimum, to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).
- Determine whether it would be applicable to use standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) once drafted.
- Investigate whether there are any approved codes of conduct or certification schemes that may be used to help you demonstrate that you have chosen a suitable processor.
- Use the ICO checklist (link below) to help you draft new contracts.

Guidance

Draft GDPR contracts guidance, ICO website **www.ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf**

Guide to the GDPR - Contracts, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/**

3.3 Information risks

Your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should set out how you (and any of your data processors) manage information risk.

You need to have a senior staff member with responsibility for managing information risks, coordinating procedures put in place to mitigate them and for logging and risk assessing information assets.

Where you have identified information risks, you should have appropriate action plans in place to mitigate any risks that are not tolerated or terminated.

Suggested actions

You should:

- Establish a clearly communicated set of security policies and procedures, which reflect business objectives and assign responsibilities to support good information risk management.
- Ensure there are processes in place to analyse and log any identified threats, vulnerabilities, and potential impacts which are associated with your business activities and information (risk register).
- Apply controls to mitigate the identified risks within agreed appetites and regularly test these controls to ensure they remain effective.

Guidance

Assessing managing risk, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/managing-risk/assessing-managing-risk/**

3.4 Data protection by design

Your business has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Under the GDPR, you have a general obligation to implement appropriate technical and organisational measures to show that you have considered and integrated data protection into your processing activities. Under the GDPR, this is referred to as data protection by design and by default.

You should adopt internal policies and implement measures which help your organisation comply with the data protection principles – this could include data minimisation, pseudonymisation and transparency measures.

Suggested actions

You should:

- Look to continually minimise the amount and type of data you collect, process and store, such as, by undertaking regular information and internal process audits across appropriate areas of the business.
- Pseudonymise the personal data where appropriate to render the data record less identifying and therefore reduce concerns with data sharing and data retention.
- Regularly undertake reviews of your public-facing documents, policies and privacy notice(s) to ensure they meet the renewed transparency requirements under the GDPR.
- Ensure any current and/or new processes or systems enable you to comply with an individual's rights under the GDPR.

- Create, review and improve your data security features and controls on an ongoing basis.

Guidance

Guide to the GDPR - Data protection by design and default, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/**

3.5 Data Protection Impact Assessments (DPIA)

Your business understands when you must conduct a DPIA and has processes in place to action this.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

DPIAs help you to identify the most effective way to comply with your data protection obligations and meet individuals' expectations of privacy.

An effective DPIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to your reputation which might otherwise occur.

You must carry out a DPIA when:

- Using new technologies.
- When the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes but is not limited to:

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- Large scale processing of special categories of data or personal data relation to criminal convictions or offences; and
- Large scale systematic monitoring of public areas.

The DPIA should contain the following information:

- A description of the processing operations and the purposes including, where applicable, the legitimate interests pursued by your business.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- Controls that you put in place to address any risks you've identified (including security).

Suggested actions

You should:

- Establish a policy which sets out when you should conduct a DPIA, who will authorise it and how it will be incorporated into the overall project plan. A DPIA screening process may be a useful tool in determining whether a DPIA is required.
- Assign responsibility for completing DPIAs to a member of staff who has sufficient control over the project to effect change e.g. Project Lead/Manager.
- Where a DPIA is required, ensure the process is completed before the project begins.
- Ensure your process for completing a DPIA includes consultation with the DPO/ data protection lead, data processors, third party contractors and with the public/their representatives in most cases.
- Ensure the information contained within the DPIA complies with the requirements under the GDPR and that the results are detailed within a report.
- Where a DPIA indicates that the processing would result in a high risk and you are unable to mitigate those risks by reasonable means, ensure your business is aware to follow the ICO consultation process to seek its opinion as to whether the processing operation complies with the GDPR.

Guidance

Guide to the GDPR - Data protection impact assessments, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/**

Your business has a DPIA framework which links to your existing risk management and project management processes.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

A DPIA can address multiple processing operations that are similar in terms of the risks, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing.

You should start to assess the situations where it will be necessary to conduct one:

- Who will do it?
- Who else needs to be involved?
- Will the process be run centrally or locally?

If the processing is wholly or partly performed by a data processor, then that processor must assist you in carrying out the DPIA. It may also be appropriate to seek the views of data subjects in certain circumstances.

Suggested actions

You should:

- Review your existing risk and project management processes and ensure there is consistency and links with your DPIA processes in place.
- Drive awareness of DPIAs across your business, and particularly amongst risk and project teams so that they understand the requirements.
- Ensure DPIA documentation is readily available for staff to use and that staff have had training on how to conduct the assessment.

3.6 Data Protection Officers

Your business has nominated a data protection lead or Data Protection Officer (DPO).

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

It is important to make sure that someone in your business, or an external data protection advisor, takes responsibility for data protection compliance.

You may need to appoint a DPO. Any business can appoint a DPO but you must do so if you:

- Are a public authority (expect for courts acting in the judicial capacity).
- Carry out large scale systematic monitoring of individuals (e.g. online behaviour tracking).
- Carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

The DPO should work independently, report to the highest management level and have adequate resources to enable your organisation meet its GDPR obligations.

The DPO's minimum tasks are to:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

Suggested actions

You should:

- Designate responsibility for data protection compliance to a suitable individual.
- Support the appointed individual through provision of appropriate training.
- Ensure there are appropriate reporting mechanisms in place between the individual responsible for data protection compliance and senior management.

- Register the details of your DPO with the ICO.
- Document the internal analysis carried out to determine whether or not a DPO is to be appointed, unless it is obvious that your organisation is not required to designate a DPO.

Guidance

Guide to the GDPR - Data protection officers, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/**

3.7 Management responsibility

Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.

- ○ Not yet implemented or planned
- ○ Partially implemented or planned
- ○ Successfully implemented
- ○ Not applicable

You should make sure that decision makers and key people in your business are aware of the requirements under the GDPR.

Decision makers and key people should lead by example, demonstrating accountability for compliance with the GDPR and promoting a positive culture, within your business, for data protection.

They should take the lead when assessing any impacts to your business and encourage a privacy by design approach.

They should help to drive awareness amongst all staff regarding the importance of exercising good data protection practices.

Suggested actions

You should:

- Clearly set out your business's approach to data protection and assign management responsibilities.
- Ensure you have a policy framework and information governance strategy in place to support a positive data protection and security culture which has been endorsed by management.
- Assess and identify areas that could cause data protection or security compliance problems and record these on your business's risk register.
- Deliver training which encourages personal responsibility and good security behaviours.
- Run regular general awareness campaigns across your business to educate staff on their data protection and security responsibilities and promote data protection and security awareness and compliance.

Guidance

Think Privacy training, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/**

Step 4 of 4: Data security, international transfers and breaches

4.1 Security policy

Your business has an information security policy supported by appropriate security measures.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should process personal data in a manner that ensures appropriate security.

Before you can decide what level of security is right for you, you will need to assess the risks to the personal data you hold and choose security measures that are appropriate to your needs.

Keeping your IT systems safe and secure can be a complex task and does require time, resource and (potentially) specialist expertise.

If you are processing personal data within your IT system(s) you need to recognise the risks involved and take appropriate technical measures to secure the data.

The measures you put in place should fit your business's needs. They don't necessarily have to be expensive or onerous. They may even be free or already available within the IT systems you currently have.

A good starting point is to establish and implement a robust information security policy which details your approach to information security, the technical and organisational measures that you will be implementing and the roles and responsibilities staff have in relation to keeping information secure.

Suggested actions

You should:

- Develop, implement and communicate an information security policy.
- Ensure the policy covers key information security topics such as network security, physical security, access controls, secure configuration, patch management, email and internet use, data storage and maintenance and security breach / incident management.
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with your security policy.
- Implement periodic checks for compliance with policy, to give assurances that security controls are operational and effective.
- Deliver regular staff training on all areas within the information security policy.

Guidance

The ICO has previously produced guidance to assist organisations in securing the personal data they hold and will be updating existing guidance to reflect GDPR provision in due course. This is a good starting point for organisations and is located in the guidance index (**www.ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications**/) under the 'security' heading.

Small businesses guidance, National Cyber Security Centre website **www.ncsc.gov.uk/smallbusiness**

4.2 International transfers

Your business ensures an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Suggested actions

You should:

- Ensure that any data you transfer outside the EU is handled in compliance with the conditions for transfer set out in Chapter V of the GDPR.
- Ensure that there is adequate safeguards and data security in place, that is documented in a written contract using standard data protection contract clauses.
- Implement measures to audit any documented security arrangements on a periodic basis.

Guidance

Guide to the GDPR - International transfers, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/**

4.3 Breach notification

Your business has effective processes to identify, report, manage and resolve any personal data breaches.

- ○ Not yet implemented or planned
- ○ Partially implemented or planned
- ○ Successfully implemented
- ○ Not applicable

The GDPR introduces a duty on all organisations to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly and without undue delay.

In all cases you must maintain records of personal data breaches, whether or not they were notifiable to the ICO.

A notifiable breach has to be reported to the ICO within 72 hours of the business becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide additional information in phases. You should make sure that your staff understand what constitutes a personal data breach, and that this is more than a loss of personal data.

You should ensure that you have an internal breach reporting procedure in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.

In light of the tight timescales for reporting a breach, it is important to have robust breach detection, investigation and internal reporting procedures in place.

Suggested actions

You should:

- Train staff how to recognise and report breaches.
- Have a process to report breaches to the appropriate individuals as soon as staff become aware of them, and to investigate and implement recovery plans.
- Put mechanisms in place to assess the likely risk to individuals and then, if necessary, notify individuals affected and report the breach to the ICO.
- Monitor the type, volume and cost of incidents to identify trends and help prevent recurrences.

Guidance

Guide to the GDPR - Data breaches, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-breaches/**

Notes

GDPR checklist for data processors

Notes

GDPR checklist for data processors

This GDPR checklist has been created by the ICO (Information Commissioners Office) to help prepare businesses for the new data protection laws due to come in to force on 25th May 2018.

We believe this to be a useful tool for our members and non-members and for all small to medium sized organisations from the private, public and third sectors.

Effective information handling makes good business sense. You will enhance your business's reputation, increase customer and employee confidence and, by making sure personal information is accurate, relevant and safe, save both time and money.

Do you process personal data as a data controller or a data processor?

Before you undertake the GDPR checklist you should first determine whether your role is as a data controller or as a data processor.

The definition of the two terms are:

Data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is, or will be, processed.

Data processor is responsible for processing personal data on behalf of a controller. If you are the data processor, the GDPR places specific legal obligations on you. For example, you will be required to maintain records of personal data and processing activities and you will have legal liability if you are responsible for a breach.

Checklist for data controllers

The process of completing the checklist will enable your business to assess your compliance with data protection law will help you to ascertain what you need to do to make sure all personal data is safe and secure.

Checklist for data processors

This section of the guide contains the checklist for a data processor only. The checklist is broken down in to four easy steps. Due to its length and detail, it is advisable to set aside plenty of time to complete all four steps effectively. To complete the checklist online, please visit **www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-processors/**

On completion, a short report will be created suggesting practical actions you can take to ensure GDPR compliance. It will also provide links to additional guidance that will help ensure your business meets the new data protection laws.

www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-controllers/

In some instances, an organisation will process personal information as both a controller and a processor. When this is the case, the ICO would advise that both checklists for a controller and processor are completed. The data controller checklist can be found on **page 13**.

Step 1 of 4: Documentation

1.1 Information you hold

Your business has conducted an information audit to map data flows.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should organise an information audit across your business or within particular business areas. One person with in-depth knowledge of your working practices may be able to do this. This will identify the data that you process and how it flows into, through and out of your business.

Remember, an information flow can include a transfer of information from one location to another. For example, the information may stay within your business yet a transfer takes place because the department or other office is located elsewhere (off site).

Having audited your information, you should then be able to identify any risks.

Suggested actions

You should:

- Organise an information audit across your business or within particular business areas to identify the data that you process and how it flows into, through and out of your business.
- Ensure this is conducted by someone with in-depth knowledge of your working practices.
- Identify and document any risks you have found, for example in a risk register.

Guidance

Find out what information you have, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/find-out-what-information-you-have/**

Identify information assets, National Archives **www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf**

Your business has documented what personal data you hold, where it came from, who you share it with and what you do with it.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Once you have completed your information audit, you should document your findings, for example, in an information asset register. Doing this will also help you to comply with the GDPR's accountability principle, which requires your business to be able to show how you comply with the GDPR principles, for example by having effective procedures and guidance for staff.

If you have **less than 250 employees** then you must keep records of any processing activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

If you have **over 250 employees**, you must record the following information:

- Name and details of your business (and where applicable, of other controllers, your representative and data protection officer).
- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Where applicable, details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- A general description of technical and organisational security measures.

You may be required to make these records available to the ICO on request.

Suggested actions

You should:

- Maintain records of processing activities detailing what personal data you hold, where it came from, who you share it with and what you do with it. This will vary depending on the size of your business.
- Consider using an information asset register to do this.
- Ensure you have procedures to guide staff on how to manage information you hold.

Guidance

Guide to the GDPR - Data protection officers, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/**

Identify information assets, National Archive **www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf**

Information Asset Register template, National Archive **www.nationalarchives.gov.uk/documents/information-management/iar_template.xls**

Step 2 of 4: Accountability and governance

2.1 Accountability

Your business has an appropriate data protection policy.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The GDPR requires you to show how you comply with the principles.

A policy will help you address data protection in a consistent manner and demonstrate accountability under the GDPR. This can be a standalone policy statement or part of a general staff policy.

The policy should clearly set out your approach to data protection together with responsibilities for implementing the policy and monitoring compliance.

The policy should be approved by management, published and communicated to all staff. You should also review and update the policy at planned intervals or when required to ensure it remains relevant.

Suggested actions

You should have a standalone policy statement or general staff policy that:

- Sets out your business's approach to data protection together with responsibilities for implementing the policy and monitoring compliance.
- Aligns with and covers the measures within this checklist as a minimum.
- Is approved by management, published and communicated to all staff.
- Is reviewed and updated at planned intervals or when required to ensure it remains relevant.

Guidance

Policy examples and templates are widely available online.

2.2 Data Protection Officers

Your business has nominated a data protection lead or Data Protection Officer (DPO).

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

It is important to make sure that someone in your business, or an external data protection advisor, takes responsibility for data protection compliance.

You may need to appoint a DPO. Any business can appoint a DPO but you must do so if you:

- Are a public authority (expect for courts acting in the judicial capacity).
- Carry out large scale systematic monitoring of individuals (e.g. online behaviour tracking).
- Carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

The DPO should work independently, report to the highest management level and have adequate resources to enable your organisation meet its GDPR obligations.

The DPO's minimum tasks are to:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

You may find it useful to designate a DPO on a voluntary basis even when the GDPR does not require you to.

You should document the internal analysis carried out to determine whether or not you appoint a DPO unless it is obvious that your business is not required to designate one.

Suggested actions

You should:

- Designate responsibility for data protection compliance to a suitable individual.
- Support the appointed individual through provision of appropriate training.
- Ensure there are appropriate reporting mechanisms in place between the individual responsible for data protection compliance and senior management.
- Register the details of your DPO with the ICO.
- Document the internal analysis carried out to determine whether or not a DPO is to be appointed, unless it is obvious that your organisation is not required to designate a DPO.

Guidance

Guide to the GDPR - Data protection officers, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/**

2.3 Management responsibility

Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should make sure that decision makers and key people in your business are aware of the requirements under the GDPR.

Decision makers and key people should lead by example, demonstrating accountability for compliance with the GDPR and promoting a positive culture, within your business, for data protection.

They should take the lead when assessing any impacts to your business and encourage a privacy by design approach.

They should help to drive awareness amongst all staff regarding the importance of exercising good data protection practices.

Suggested actions

You should:

- Clearly set out your business's approach to data protection and assign management responsibilities.
- Ensure you have a policy framework and information governance strategy in place to support a positive data protection and security culture which has been endorsed by management.
- Assess and identify areas that could cause data protection or security compliance problems and record these on your business's risk register.
- Deliver training which encourages personal responsibility and good security behaviours.
- Run regular general awareness campaigns across your business to educate staff on their data protection and security responsibilities and promote data protection and security awareness and compliance.

Guidance

Think Privacy training, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/**

2.4 Information risks and data protection impact assessments

Your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.

- ○ Not yet implemented or planned
- ○ Partially implemented or planned
- ○ Successfully implemented
- ○ Not applicable

You should set out how you manage information risk.

This task could be driven by the data controller you are providing services for and you should ensure you work with this controller to ensure that all information risks you identify are fed back on a regular basis.

You need to have a senior staff member with responsibility for managing information risks, coordinating procedures put in place to mitigate them and for logging and risk assessing information assets.

Where you have identified information risks, you should have appropriate action plans in place to mitigate any risks that are not tolerated or terminated.

Before the start of a new contract with you, the data controller should complete a Data Protection Impact Assessment (where the circumstances require one to be completed) – as data processor you should be ready to provide your input to this assessment and work with the controller to mitigate any risks identified. Having an established information risk management framework in place will assist you to do this effectively.

Suggested actions

You should:

- Establish a clearly communicated set of security policies and procedures, which reflect business objectives and assign responsibilities to support good information risk management.
- Ensure there are processes to analyse and log any identified threats, vulnerabilities, and potential impacts which are associated with your business activities and information (risk register).
- Apply controls to mitigate the identified risks within agreed appetites and regularly test these controls to ensure they remain effective.
- Work with the data controller to ensure that all information risks you identify are fed back on a regular basis.
- Provide your input to any data protection impact assessments (DPIAs) that the data controller may initiate before the start of the contract with you, or at the point where any significant changes are needed.
- Work with the controller to mitigate any risks identified as part of the DPIA.

Guidance

Data protection impact assessments, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/**

Assessing and managing risk, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/managing-risk/assessing-managing-risk/**

2.5 Data protection by design

Your business has implemented appropriate technical and organisational measures to show you have considered and integrated data protection into your processing activities.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Under the GDPR, data processors have a general obligation to implement technical and organisational measures to show that they have considered and integrated data protection into their processing activities. Under the GDPR, this is referred to as data protection by design and by default.

You should adopt internal policies and implement measures which help your business comply with the data protection principles – this could include data minimisation, pseudonymisation and transparency measures.

Suggested actions

You should:

- Look to continually minimise the amount and type of data you collect, process and store, such as by undertaking regular information and internal process audits across appropriate areas of the business.
- Pseudonymise the personal data where appropriate to render the data record less identifying and therefore reduce concerns with data sharing and data retention.
- Regularly undertake reviews of your public-facing documents, policies and privacy notice(s) to ensure they meet the renewed transparency requirements under the GDPR.
- Ensure any current and/or new processes or systems enable you to comply with an individual's rights under the GDPR.
- Create, review and improve your data security features and controls on an ongoing basis.

Guidance

Guide to the GDPR - Data protection by design and default, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/**

2.6 Training and awareness

Your business provides data protection awareness training for all staff.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should brief all staff handling personal data on their data protection responsibilities. It is good practice to provide awareness training on or shortly after appointment with updates at regular intervals or when required.

You should also consider specialist training for staff with specific duties, such as information security and database management and marketing.

The regular communication of key messages is equally important to help reinforce training and maintain awareness (for example intranet articles, circulars, team briefings and posters).

Suggested actions

You should:

- Provide induction training on or shortly after appointment.
- Update all staff at regular intervals or when required (for example, intranet articles, circulars, team briefings and posters).
- Provide specialist training for staff with specific duties, such as marketing, information security and database management.

Guidance

Think privacy toolkit, ICO website **www.ico.org.uk/for-organisations/improve-your-practices/posters-stickers-and-e-learning/**

Training checklist for small to medium sized organisations, ICO website **www.ico.org.uk/media/for-organisations/documents/1606/training-checklist.pdf**

2.7 The use of sub-processors

Your business has sought prior written authorisation from the data controller before engaging the services of a sub-processor.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should only engage another processor if you have the prior written authorisation of the data controller. This authorisation may be specific or general. However, if the authorisation is general, then, as data processor, you must tell the controller in advance of any changes you intend to make regarding the addition or replacement of other processors, so that they have the opportunity to object.

You should ensure this is included as a standard contract term.

Data processors now have responsibilities and liabilities in their own right, and processors as well as controllers may now be liable for penalties under the GDPR.

In the future, you may wish to consider looking at approved codes of conduct or certification schemes to help you demonstrate your suitability as a data processor. Standard contractual clauses may form part of such a code or scheme.

Suggested actions

You should:

- Seek written authorisation from the data controller before entering into any form of agreement or engagement of services of a sub-processor.
- Ensure you have a written contract or agreement in place with the sub-processor which outlines the data protection arrangements and expectations (such as staff training, data retention, data destruction, data access and breach reporting) the sub-processor must have in place.
- Make sure any data is shared securely with the sub-processor and that you obtain the relevant assurances that the sub-processor has implemented appropriate technical and organisational measures to ensure the security of the personal data they are processing on your behalf.
- Ensure that if there are any changes in the sub-processor agreements that authorisation is again sought from the data controller before any changes are made.

Guidance

Draft contracts guidance, ICO website **www.ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf**

2.8 Operational base

If your business operates outside the EU, you have appointed a representative within the EU in writing.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Under the GDPR, if your business is located outside the EU, and you offer products and services to citizens in the EU, then there is a requirement for you to appoint (in writing) a representative within the European Union.

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Suggested actions

You should:

- Appoint (in writing) a representative within the European Union.
- Ensure your contract with the data controller meets all the conditions for transfer of personal data outside of the EU set out in Chapter V of the GDPR.

2.9 Breach notification

Your business has effective processes to identify, report, manage and resolve any personal data breaches.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The GDPR introduces a duty on all data processors to inform controllers of a personal data breach "without undue delay" after becoming aware of it, which is why it is important that you have an internal and external breach identification and reporting procedures in place.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

You should make sure that your staff understand what constitutes a data breach, and that this is more than a loss of personal data.

You should have investigation procedures in place to ensure that you can assist the controller in its responsibilities to act when a data breach occurs.

Suggested actions

You should:

- Have a process to enable breaches to be reported to management as soon as staff become aware of them, and to investigate and implement recovery plans.
- Put mechanisms in place to assess and then report any breaches to the data controller.
- Monitor the type, volume and cost of incidents to identify trends and help prevent recurrences.

Guidance

Guide to the GDPR - Data breaches, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-breaches/**

Guidelines on personal data breach notification under Regulation 2016/679, Article 29 Working Party **www.ec.europa.eu/newsroom/document.cfm?doc_id=47741**

Step 3 of 4: Individual rights

3.1 Right of access

Your business has a process to respond to a data controller's request for information (following an individual's request to access their personal data).

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Individuals have the right to obtain:

- Confirmation that their data is being processed.
- Access to their personal data.
- Other supplementary information – this largely corresponds to the information that you should be provide in a privacy notice.

If you have identified and documented all the data you process it will make it easier to locate and retrieve specific information at the request of the data controller, as information must be provided by the data controller without delay and at the latest within one month of receipt of the request. You should have robust procedures in place and assign responsibility within your business to deal with these types of requests in a timely manner.

If the request is made electronically, you may be required by the data controller to send them the information in a commonly used electronic format.

Timescales for your response to a request for an individual's information should be set within the written contract with the data controller.

Suggested actions

You should:

- Ensure a process is in place to allow you to respond to the data controller's request for information (in relation to a subject access request they have received from an individual) in line with the agreed contractual SLA obligations and in order for the data controller to meet statutory timescales.
- Include subject access procedures within your written data protection policy.
- Provide appropriate awareness training to all staff and more specialised training to individuals that will be dealing with any requests.

Guidance

Guide to the GDPR - Right of access, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/**

3.2 Right to rectification and data quality

Your business has processes to ensure that the personal data you hold remains accurate and up to date.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

If you have identified and documented all the data you process it will make it easier to locate and retrieve specific information at the request of the data controller, as information must be provided by the data controller without delay and at the latest within one month of receipt of the request. You should have robust procedures in place and assign responsibility within your business to deal with these types of requests in a timely manner.

If the request is made electronically, you may be required by the data controller to send them the information in a commonly used electronic format.

Timescales for your response to a request for an individual's information should be set within the written contract with the data controller.

Suggested actions

You should:

- Have procedures to respond to a request from a data controller to correct inaccurate records.
- Create records management policies, with rules for creating and keeping records (including emails).
- Conduct regular data quality reviews of systems and manual records you hold to ensure the information continues to be adequate for the purposes of processing (for which it was collected).
- Regularly review information to identify when you need to correct inaccurate records, remove irrelevant ones and update out-of-date ones.
- Promote and feedback any data quality trends to staff through ongoing awareness campaigns and internal training.

Guidance

Guide to the GDPR - Right to rectification, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/**

3.3 Right to erasure including retention and disposal

Your business has a process to routinely and securely dispose of personal data that is no longer required in line with agreed timescales as stated within your contract with the data controller.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Individuals have the right to be forgotten and can request the data controller (and therefore you also as data processor) to erase their personal data when:

- It is no longer necessary in relation to the purpose for which it was originally collected/ processed.
- The individual withdraws consent.
- The individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- It was unlawfully processed (i.e. otherwise in breach of the GDPR).
- It has to be erased in order to comply with a legal obligation.
- It is processed in relation to the offer of information society services to a child.

These requests will be received initially by the data controller however, if the data in question is also processed or stored by you, then you will need to have the appropriate procedures in place in order to ensure the data is erased permanently.

You should have standard contract clauses covering erasure, data retention and disposal. You should ensure that these conditions are met. A written retention policy will remind you when to dispose of various categories of data, and help you plan for its secure disposal.

Suggested actions

You should:

- Ensure your written contract with the data controller includes standard contract clauses covering data erasure, retention and disposal.
- Have processes in place to ensure that these conditions are met.
- Consider creating a written retention policy to remind you when to dispose of various categories of data, and help you plan for its secure disposal.
- Should you receive a request from the data controller to erase an individual's personal data, have appropriate procedures in place in order to ensure the data is erased permanently.

Guidance

Disposal of Records, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/**

3.4 Right to restrict processing

Your business has procedures to respond to a data controllers' request to supress the processing of specific personal data.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Individuals have a right to block or restrict the processing of personal data.

When processing is restricted, you are permitted to store the personal data, but not further process it.

You can retain just enough information about the individual to ensure that the restriction is respected in the future.

A data controller may request that as their data processor you restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the data controller is considering whether their legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If the data controller no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Suggested actions

You should:

- Ensure you have processes in place to act on any request from the data controller to restrict the processing of an individual's personal data.

Guidance

Guide to the GDPR - Right to restrict processing, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/**

3.5 Right of data portability

Your business can respond to a request from the data controller for the supply of the personal data you process in an electronic format.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

They can receive personal data or move, copy or transfer that data from one business to another in a safe and secure way, without hindrance.

The right to data portability only applies:

- To personal data an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.
- Where the processing is carried out by automated means.

Information must be provided without delay and at least within one month of receipt. Your data controller may receive such a request and so you should be able to supply them with any applicable data you process on their behalf to enable them to fulfil the request.

You must provide the personal data in a structured, commonly used and machine readable format. Examples of appropriate formats include CSV and XML files.

If the individual (and so the data controller) requests it, you may be required to transmit the data directly to another business where this is technically feasible.

Suggested actions

You should:

- Ensure you have a process in place to enable you to respond to any request from the data controller for the provision of data you process in a structured, commonly used and machine readable form.
- Ensure that the medium in which the data is provided has appropriate technical security controls in place to protect the data it contains.

Guidance

Guide to the GDPR - Right to data portability, ICO website **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/**

Step 4 of 4: Data security

4.1 Security policy

Your business has an information security policy supported by appropriate security measures.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should process personal data in a manner that ensures appropriate security.

Before you can decide what level of security is right for you, you will need to assess the risks to the personal data you hold and choose security measures that are appropriate to your needs. Keeping your IT systems safe and secure can be a complex task and does require time, resource and (potentially) specialist expertise.

If you are processing personal data within your IT system(s) you need to recognise the risks involved and take appropriate technical measures to secure the data.

The measures you put in place should fit your business's needs. They don't necessarily have to be expensive or onerous. They may even be free or already available within the IT systems you currently have.

A good starting point is to establish and implement a robust Information Security policy which details your approach to information security, the technical and organisational measures that you will be implementing and the roles and responsibilities staff have in relation to keeping information secure.

Suggested actions

You should:

- Develop, implement and communicate an Information Security policy.
- Ensure the policy covers key information security topics such as network security, physical security, access controls, secure configuration, patch management, email and internet use, data storage and maintenance and security breach / incident management.
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with your security policy.
- Implement periodic checks for compliance with policy, to give assurances that security controls are operational and effective.
- Deliver regular staff training on all areas within the Information Security policy.

Guidance

The ICO has previously produced guidance to assist organisations in securing the personal data they hold. We are working to update existing guidance to reflect GDPR provisions and once completed, this section will expand to include this information.

In the meantime, the existing guidance is a good starting point for organisations. This is located in the **guidance index** (**www.ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/**) under the 'security' heading.

Small businesses guidance, National Cyber Security Centre website **www.ncsc.gov.uk/smallbusiness**

GDPR checklist for data sharing and subject access

Notes

GDPR checklist for data sharing and subject access

This GDPR checklist has been created by the ICO (Information Commissioners Office) to help prepare businesses for the new data protection laws due to come in to force on 25th May 2018. We believe this to be a useful tool for our members and non-members and for all small to medium sized organisations from the private, public and third sectors.

Effective information handling makes good business sense. You will enhance your business's reputation, increase customer and employee confidence and, by making sure personal information is accurate, relevant and safe, save both time and money.

Checklist for businesses involved in data sharing and subject access.

GDPR covers the data sharing and subject access as part of the new data protection laws. This checklist is designed to help you assess your organisation's data sharing policies and agreements, compliance monitoring, maintaining sharing records, registration and your process for how to deal with a subject access request.

If you would like to complete this online checklist please visit **www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/**

On completion, a short report will be created suggesting practical actions you can take to ensure you are compliant with the GDPR. It will also provide links to additional guidance that will help ensure your business meets the new data protection laws.

Do you process personal data as a data controller or a data processor?

Before you undertake the GDPR checklist you should first determine whether your role in the process is as a data controller or as a data processor.

The definition of the two terms are:

Data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which any personal data is, or will be, processed.

Data processor is responsible for processing personal data on behalf of a controller. If you are data processor, the GDPR places specific legal obligations on you. For example, you will be required to maintain records of personal data and processing activities and you will have legal liability if you are responsible for a breach.

In some instances, an organisation will process personal information as both a data controller and a data processor. When this is the case, the ICO would advise that both assessments for a controller and processor are completed. Access to both checklists can be found here:

www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

Step 1 of 5: Management and organisational data sharing

1.1 Data sharing policy

Your business has communicated policies, procedures and guidance to all staff which clearly set out when it is appropriate to share or disclose data.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Your policies, procedures and guidance should set out how staff ought to respond to sharing requests in the appropriate manner. Data sharing must be done in a way that complies with the law, is fair, transparent and in line with the rights and expectations of the people whose data is being shared. Your policy should explain how compliance with these requirements will be achieved e.g. monitoring of information, sharing logs, quality assessment of samples, and instances of sharing.

This policy should be communicated to all relevant staff e.g. via intranet.

Areas for focus and suggested actions

Your policies, procedures and guidance should set out how staff ought to respond to sharing requests in the appropriate manner.

You should:

- Have an appropriate policy in place setting out when it is appropriate to share and/or disclose data.
- Ensure your policy and processes have considered how staff will ensure that sharing is legal, how the accuracy of the data will be maintained and what security measures should be put in place prior to any sharing of information.
- Detail in your policy how compliance with these requirements will be achieved.
- Communicate the policy framework to all staff.

Guidance

Data sharing checklist, ICO **www.ico.org.uk/media/for-organisations/documents/1067/data_sharing_checklists.pdf**

Governance, in ICO data sharing code of practice **www.ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf**

1.2 Accountability

Your business has assigned responsibility to an appropriate member of staff for ensuring effective data sharing.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

It is good practice to nominate a senior, experienced person to take on overall responsibility for information sharing, ensuring compliance with the law, and providing advice to staff making decisions about sharing. Your policy should make it clear who this person is and how they can be contacted. The nominated individual should also receive appropriate specialist training to allow them to fulfil this role.

Areas for focus and suggested actions

It is good practice to nominate a senior, experienced person to take on overall responsibility for information sharing, ensuring compliance with the law, and providing advice to staff faced with making decisions about such sharing.

You should:

- Appoint a suitable senior experienced person(s) and ensure the role is detailed within the policy.
- Provide suitable training to the individual(s) to enable them to fulfill the role.

Guidance

Governance, in ICO data sharing code of practice **www.ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf**

1.3 Staff training

Your business provides adequate training on an ongoing basis for staff that are regularly required to make decisions regarding whether or not personal data should be shared with third parties.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

It is essential to provide appropriate training to staff who are likely to make significant decisions about data sharing or have access to shared data. The nature of the training will depend on their role within the sharing process. Such training can be incorporated into any training you already give on data protection, security, or legal obligations of staff. Once delivered effort should be made to maintain that awareness. Materials such as posters, office wide emails, intranet updates or data sharing content in newsletters could be employed to achieve this.

Areas for focus and suggested actions

It is essential to provide appropriate training to staff who are likely to make significant decisions about data sharing or have access to shared data. The nature of the training will depend on their role within the sharing process.

You should:

- Provide adequate training on an ongoing basis for staff who are regularly required to make decisions regarding whether or not personal data should be shared with third parties.
- Ensure staff with specific responsibility for management or oversight of information sharing processes complete appropriate training to allow then to fulfil this role.
- Maintain staff awareness through materials such as posters, office wide emails, intranet updates or data sharing content in newsletters.

Guidance

Governance, in ICO Data sharing code of practice **www.ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf**

Step 2 of 5: Data sharing records

2.1 Decision log

Your business maintains a log of all decisions to share personal data and this is reviewed regularly.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Your business should be able to justify the reasons why you decided to share specific personal data. Such sharing should be lawful and comply with any statutory restrictions in place on your organisation.

When a decision has been made regarding whether to share information or not you should record your decision and your reasoning (regardless of if you shared information) along with what information was shared and for what purpose, who it was shared with, when it was shared and if the information was shared with or without consent.

You should review the log of sharing decisions on a regular basis to ensure that decisions to share data are well founded and compliant. You should also use the review to identify areas where large quantities of data are being shared routinely and whether there is a need to formalise this with an information sharing agreement, if one is not in place already.

Areas for focus and suggested actions

Your business should be able to justify the reasons why you decided to share specific personal data. Such sharing should be lawful and comply with any statutory restrictions in place on your organisations. In addition there should be an appropriate legal basis under one of the gateways or "conditions for processing" set out in schedules 2 and 3 of the Data Protection Act unless a relevant exemption from the DPA applies.

You should:

- Maintain a log of all decisions to share personal data. Review it regularly to ensure that decisions to share data are well founded and compliant. This also helps to identify areas where large quantities of data are being shared routinely and, therefore, there is a need to formalise this with an information sharing agreement.
- Where you are sharing data routinely, implement appropriate data sharing agreements (DSA) with all parties which are reviewed on a regular basis and recorded on a central DSA Log.

Guidance

How do we decide the legal basis for sharing?, Centre of Excellence for Data Sharing **www.informationsharing.org.uk/our-work/tools/scoping/how-do-we-decide-the-legal-basis-for-sharing/**

Conditions for processing, in ICO data sharing code of practice **www.ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf**

Guidance on how to record decisions about whether or not information is shared, Department of Education **www.informationsharing.co.uk/wp-content/uploads/2012/08/DfE-how-to-record-decisions.pdf**

Data sharing decision" form, in ICO data sharing code of practice **www.ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf**

2.2 Information sharing agreements

Your business has agreed data sharing agreements with an appropriate legal basis with all parties with whom personal data is routinely shared or where large quantities of data are to be transferred. These agreements are regularly reviewed.

- ○ Not yet implemented or planned
- ○ Partially implemented or planned
- ○ Successfully implemented
- ○ Not applicable

In order to ensure that personal data is managed effectively and securely it is necessary for you to know what information you hold and how. As such it may be necessary to carry out an 'information audit' or 'records survey' to identify records and data sets held by the organisation.

This process will help in determining which business functions create certain records, which records are vital to the functioning of the business, where they are kept, how long they are kept for and who needs to use them now and in the future.

Once this information is gathered it may allow for the development of retention and disposal schedules, improved security practices and the development of disaster recovery processes.

Areas for focus and suggested actions

In some instances, you may need to agree and regularise the way you share personal data. This may become clear from the volume of ad hoc requests you receive from a particular organisation or due to the introduction of a new process which will require the sharing of large quantities of data.

You should:

- Complete a legal compliance assessment prior to introducing a new information sharing agreement to ensure that your business has legal authority to share the information and that such sharing complies with the requirements of the Data Protection Act 1998.
- Regularly review information sharing arrangements to ensure they still reflect the current needs of your business and are compliant with the DPA. Such reviews should address whether the data is still needed to fulfil the purposes for which it is being shared and whether the ISA reflect current data sharing arrangements.

Guidance

Governance, in ICO data sharing code of practice **www.ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf**

How do we decide the legal basis for sharing?, Centre of Excellence for Data Sharing **www.informationsharing.org.uk/our-work/tools/scoping/how-do-we-decide-the-legal-basis-for-sharing/**

How do we agree and implement an information sharing agreement?, Centre of Excellence for Data Sharing **www.informationsharing.org.uk/our-work/tools/pre-implementation/how-do-we-agree-and-implement-an-information-sharing-agreement/**

Reviewing your data sharing arrangements, in ICO data sharing code of practice **www.ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf**

Step 3 of 5: Registration

3.1 Fair processing

Your business informs individuals about the sharing of their personal data.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The first principle of the DPA requires that you process personal data fairly and lawfully. In order for the sharing of personal data to be considered fair you need to explain to individuals how you will use their personal data and who you will share it with. It is good practice to include privacy notices on your website and any forms that you use to collect data. These should clearly explain the reasons for using the data including any disclosures or sharing.

The second principle of the DPA requires that you do not process personal data in any manner that is 'incompatible' with your specified purposes. In practice, this means that if you want to use or share personal data for a reason that was not covered in your privacy notice you should consider obtaining prior consent to ensure the new use is fair.

Areas for focus and suggested actions

In order for the sharing of personal data to be considered fair and lawful the *Data Protection Act 1998* imposes a requirement on organisations to explain to individuals how they will use personal data which they collect and who they will share it with. In such data sharing contexts it is important to explain:

- Who you are.
- Why you are going to share personal data.
- Who you are going to share it with – this could be actual named organisations or types of organisation.
- Provide further information if the situation where the nature of the sharing is such that some aspects of it would not be in the "reasonable expectations" of the individual and that you would use their data in that way in order to allow the sharing to be considered fair.

Guidance

Collecting information about your customers checklist, ICO **www.ico.org.uk/media/for-organisations/documents/1584/pn_collecting_information_small_business_checklist.pdf**

Privacy notices code of practice, ICO **www.ico.org.uk/media/for-organisations/documents/1610/privacy_notices_cop.pdf**

3.2 ICO registration

Your business has considered whether you need to provide the Information Commissioner's Office (ICO) with a description of the individuals or organisations to whom you intend or may wish to disclose personal data.

- ○ Not yet implemented or planned
- ○ Partially implemented or planned
- ○ Successfully implemented
- ○ Not applicable

If you process personal data you may need to record the types of data you hold and why on the public register of data controllers. This is called 'registration'.

This registration should include details of other organisations or groups of organisations you intend to share personal data with. Your business should ensure that these details are kept up to date.

Areas for focus and suggested actions

Most organisations are required by statute to provide the ICO with certain details regarding their processing of personal information. When you intend to share personal data with another organisation or group of organisations, you should:

- Check whether you need to update your ICO registration to describe this. When any part of the registration entry becomes inaccurate or incomplete, for example, because you are now disclosing information to a new type of organisation, you must inform the ICO as soon as practical and in any event within 28 days. It is a criminal offence not to do this.

Guidance

Register (notify) under the Data Protection Act, ICO **www.ico.org.uk/for-organisations/register/**

Registration self assessment, ICO **www.ico.org.uk/for-organisations/register/self-assessment/**

Registration FAQs, ICO **www.ico.org.uk/for-organisations/register/faqs/**

Notification exemptions - a self-assessment guide to data protection, ICO **www.ico.org.uk/for-organisations/register/self-assessment/**

Step 4 of 5: Security

4.1 Security measures

Your business has appropriate security measures in place to protect data in transit, received by your business and transferred to another business.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The DPA requires organisations to have appropriate technical and organisational measures in place to protect shared personal data. In some instances you may transfer personal data to another organisation but still remain responsible for its security. It is therefore important that you set out, and ensure compliance with, agreed levels of security in relation to the personal data being shared.

Please see our information security checklist for hints and tips on how to improve the security of personal data held by your organisation.

In addition, when transferring data between organisations, appropriate measures should be taken to ensure the security of that data while in transit. This may include the use of encryption on email, secure file transfer protocol (SFTP) or Virtual Private Network (VPN) for electronic files. Equally there should be equivalent security around paper documents in transit. Such controls might include the use of a reliable courier, other secure postage and use of locked containers or tamper evident packaging.

Areas for focus and suggested actions

The Data Protection Act (DPA) requires organisations to have appropriate technical and organisational measures in place to protect shared personal data. In some instances you may transfer personal data to another organisation but still remain responsible for its security.

You should:

- Always use an appropriate form of transport e.g. secure courier for sensitive paper based personal data and encryption on email, secure file transfer protocol (SFTP) or Virtual Private Network (VPN) for electronic files.
- Minimise data being transported.
- Log the transfer in and out where appropriate and check to ensure that data is received.
- Employ security measures to safeguard the data in transit such as tamper evident packaging and storage on encrypted devices.

Guidance

ICO data sharing code of practice, page 23 **www.ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf**

Step 5 of 5: Subject access

5.1 Subject access process

Your business has a documented process for processing subject access requests which has been effectively implemented. Your business has measures in place to ensure requests are appropriately recognised, timescales are met and the appropriate information is provided.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should assign responsibility for responding to subject access requests to one or more individuals.

You should have a documented process for processing subject access requests efficiently and in accordance with the DPA.

The documented process should be approved by senior management and made readily available to staff.

Suggested actions

Responsibility for responding to subject access requests should be assigned to one or more individuals.

You should:

- Implement a documented process for processing subject access requests efficiently and in accordance with the DPA.

- Ensure the documented process has been approved by senior management and made readily available to personnel.

Guidance

How do I handle subject access requests, in ICO subject access requests code of practice **www.ico.org.uk/media/for-organisations/documents/1599/subject-access-checklist.pdf**

Subject access requests code of practice, ICO **www.ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf**

5.2 Accountability and training

Your business has appropriately resourced and trained all personnel assigned responsibility for processing subject access requests. Your business has made all personnel aware of their responsibility to support subject access requests and where in the organisation they should direct requests to.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

All staff should be briefed on their responsibilities in relation to the identifying, processing and escalating subject access requests on or shortly after appointment with updates at regular intervals thereafter to maintain levels of awareness. Awareness materials might include posters, office wide emails, intranet updates and newsletters.

Staff with specific subject access request responsibilities such as processing, logging or overseeing responses to subject access requests should receive appropriate training in order to allow them to carry out their role effectively.

Areas for focus and suggested actions

Your business should brief all staff on their responsibilities for identifying, processing and escalating subject access requests.

You should:

- Provide appropriate training as part of any induction training on or shortly after appointment.
- Ensure all staff receive updates and refresher training at regular intervals thereafter to maintain levels of awareness.
- Utilise awareness materials such as posters, office wide emails, intranet updates, newsletters.
- Give staff with specific subject access request responsibilities (such as processing, logging or overseeing responses) appropriate training on subject access requests in order to allow them to carry out their role effectively.

Guidance

How do I handle subject access requests, in ICO subject access requests code of practice **www.ico.org.uk/media/for-organisations/documents/1599/subject-access-checklist.pdf**

Subject access requests code of practice, ICO **www.ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdfc**

5.3 Compliance monitoring

The process monitors and reviews and, where necessary, additional measures have been implemented to improve compliance.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should periodically review the documented process and, where appropriate, update it to ensure it remains adequate and relevant.

You should have mechanisms in place to regularly monitor and report on agreed performance measures and apply any recommendations or lessons learned.

Your business should consider maintaining records showing measures and reporting, e.g. management information/KPI, meeting minutes, emails, etc. Compliance checks and audits could be introduced to demonstrate any reviews of process.

Areas for focus and suggested actions

It is important to monitor compliance to policy therefore you should:

- Periodically review the documented process and, where appropriate, update it to ensure it remains adequate and relevant.
- Put mechanisms in place to regularly monitor and report on agreed performance measures and any recommendations or lessons learned are applied.
- Consider maintaining records showing measures and reporting, e.g. management information/KPI, meeting minutes, emails, etc.

Guidance

How do I handle subject access requests?, ICO **www.ico.org.uk/media/for-organisations/documents/1599/subject-access-checklist.pdf**

Subject access code of practice, ICO **www.ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf**

Notes

GDPR checklist for information security

Notes

GDPR checklist for information security

This GDPR checklist has been created by the ICO (Information Commissioners Office) to help prepare businesses for the new data protection laws due to come in to force on 25th May 2018. We believe this to be a useful tool for our members and non-members and for all small to medium sized organisations from the private, public and third sectors.

Effective information handling makes good business sense. You will enhance your business's reputation, increase customer and employee confidence and, by making sure personal information is accurate, relevant and safe, save both time and money.

Checklist for businesses involved in information security.

GDPR covers the data sharing and subject access as part of the new data protection laws. This checklist enables you to assess your compliance in the specific areas of information and cyber security policy and risk, mobile and home working, removable media, access controls and malware protection.

If you would like to complete this online checklist please visit **www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/**

On completion, a short report will be created suggesting practical actions you can take to ensure you are compliant with the GDPR. It will also provide links to additional guidance that will help ensure your business meets the new data protection laws.

Do you process personal data as a data controller or a data processor?

Before you undertake the GDPR checklist you should first determine whether your role in the process is as a data controller or as a data processor.

The definition of the two terms are:

Data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is or will be processed.

Data processor is responsible for processing personal data on behalf of a controller. If you are the processor, the GDPR places specific legal obligations on you. For example, you will be required to maintain records of personal data and processing activities and you will have legal liability if you are responsible for a breach.

In some instances, an organisation will process personal information as both a data controller and a data processor. When this is the case, the ICO would advise that both assessments for a controller and processor are completed. Access to both checklists can be found here:

www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

Step 1: Management and organisation information security

1.1 Risk management

Your business has established a process to identify, assess and manage information security risks. Your business ensures information security risks are assessed and appropriately managed.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Before you can establish what level of security is right for your business you will need to review the personal data you hold and assess the risks to that information.

You should consider all processes involved as you collect, store, use, share and dispose of personal data. Also, consider how sensitive or confidential the data is and what damage or distress could be caused to individuals, as well as the reputational damage to your business, if there was a security breach.

With a clearer view of the risks you can begin to choose the security measures that are appropriate for your needs.

Areas for focus and suggested actions

Before you can establish what level of security is right for your business you will need to review the personal data you hold and assess the risks to that information.

You should:

- Consider all processes involved as you collect, store, use, share and dispose of personal data.
- Consider how sensitive or confidential the data is and what damage or distress could be caused to individuals, as well as the reputational damage to your business, if there was a security breach.

With this clearer view of the risks you can then implement the following:

- Document your information risk management process in an information risk policy.
- Ensure that you create either a stand alone information risk register or incorporate information risks in a central risk register.
- Regularly assess and update, treat, tolerate, or mitigate risks as appropriate.

Guidance

Information risk management regime, in 10 steps to cyber security, National Cyber Security Centre **www.ncsc.gov.uk/guidance/10-steps-information-risk-management-regime**

1.2 Information security policy

Senior management has approved and published an appropriate information security policy. Your business provides management direction and support for information security in accordance with business needs and relevant laws and regulations.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

A policy will enable you to address security risks in a consistent manner. This can be part of a general policy or a standalone policy statement that is supported by specific policies.

The policy should clearly set out your business' approach to security together with responsibilities for implementing the policy and monitoring compliance.

You or your business should have a process in place to ensure that information security related policies and procedures are reviewed and approved before implementation.

You should then give policies and procedures, set review dates and review and update in line with agreed timescales or when required.

It is good practice to have a document in place, which outlines the agreed style that all policies, procedures and guidance documents must follow which you then have communicated to relevant managers and staff.

Areas for focus and suggested actions

A policy will enable you to address security risks in a consistent manner. This can be part of a general policy or a standalone policy statement that is supported by specific policies.

You should:

- Implement an Information Security policy that covers all aspects of information security within your organisation.
- Ensure the policy clearly sets out your business' approach to security together with responsibilities for implementing the policy and monitoring compliance.
- Set review dates and ensure policies and procedures are reviewed and updated in line with agreed timescales or when required.

Guidance

Information security, ICO Guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/**

Staff policies, Get Safe online website **www.getsafeonline.org/businesses/staff-policies/**

1.3 Information security responsibility

Your business has defined and allocated information security responsibilities. Your business has established a management framework to coordinate and review the implementation of information security.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

It is good practice to identify a person or department in your business with day-to-day responsibility for developing, implementing and monitoring the security policy. They should have the necessary authority and resources to fulfil this responsibility effectively.

For larger organisations, it is common to appoint 'owners' with day-to-day responsibility for the security and use of business systems.

Areas for focus and suggested actions

Without clear accountability for the security of systems and specific processes, your overall security will not be properly managed or coordinated and will quickly become flawed and out of date.

You should:

- Identify a person or department in your business and assign day-to-day responsibility for information security.
- Ensure they have the necessary authority and resources to fulfil this responsibility effectively.
- For larger organisations, appoint 'owners' with day-to-day responsibility for the security and use of business systems.

Guidance

Information security, in ICO Guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/**

The National Cyber Security Centre (NCSC) guidance for small businesses **www.ncsc.gov.uk/smallbusiness**

1.4 Outsourcing

Your business has established written agreements with third party service providers that include appropriate information security conditions. Your business ensures the protection of personal data that is accessed by suppliers and providers.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Many small businesses outsource some or all of their data processing requirements to hosted (including cloud based) services. You must be satisfied that these 'data processors' will treat your information securely as your business will remain responsible for ensuring the processing complies with the DPA.

You must choose a provider that gives sufficient guarantees about its security measures. For example, you might review copies of any security assessments and, where appropriate, visit their premises to make sure they have appropriate security arrangements in place.

You must also have a written contract setting out what the provider is allowed to do with the personal data and requiring them to take the same security measures you would have to take to comply with the DPA.

If you use a provider to erase data and dispose of or recycle your ICT equipment, make sure they do it adequately. You will be held responsible if personal data collected by you is extracted from your old equipment if it is resold.

Areas for focus and suggested actions

Many small businesses outsource some or all of their data processing requirements to hosted (including cloud based) services. You should be satisfied that these 'data processors' will treat your information securely as your business will be held responsible under the DPA for what they do with the personal data. Therefore, you should:

- Ensure data processors will treat your information securely - establish data processing contracts where feasible and ensure they contain necessary data protection related clauses.
- Establish protocols to allow periodic security reviews of the security arrangements in place to provide assurances of compliance to contract/agreement.
- If you use a provider to erase data and dispose of or recycle your ICT equipment, make sure they do it adequately. You may be held responsible if personal data collected by you is extracted from your old equipment when it is resold.

Guidance

Information security, ICO Guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/**

Outsourcing, ICO **www.ico.org.uk/media/for-organisations/documents/1585/outsourcing_guide_for_smes.pdf**

Cloud computing, ICO w**ww.ico.org.uk/for-the-public/online/cloud-computing/**

IT asset disposal, ICO **www.ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf**

Model contract clauses: International transfers of personal data, ICO **www.ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf**

Model contracts for the transfer of personal data to third countries, European Commission website **www.ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en**

Data controllers and data processors: what the difference is and what the governance implications are, ICO **www.ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf**

1.5 Incident management

Your business has established a process to report and recover from data security breaches. Your business ensures the management of data security breaches, including communication of information security events and weaknesses.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Data security breaches may arise from a theft, an attack on your systems, the unauthorised use of personal data by a member of staff, or from accidental loss or equipment failure.

However a breach occurs it is important that you deal with it effectively and learn from it. You should have a process to report breaches to management as soon as staff become aware of them, and to investigate and implement recovery plans.

Ideally, you should monitor the type, volume and cost of incidents to identify trends and help prevent recurrences.

Areas for focus and suggested actions

Data security breaches may arise from a theft, an attack on your systems, the unauthorised use of personal data by a member of staff, or from accidental loss or equipment failure. However a breach occurs it is important that you deal with it effectively and learn the lessons and therefore you should:

- Have a process to report breaches to management as soon as staff become aware of them and to investigate and implement recovery plans.
- Monitor the type, volume and cost of incidents to identify trends and help prevent recurrences.

Guidance

Notification of data security breaches to the ICO, ICO **www.ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/**

Incident management, in 10 steps to cyber security, National Cyber Security Centre **www.ncsc.gov.uk/guidance/10-steps-incident-management**

Step 2 of 4: Your staff and information security awareness

2.1 Training and awareness

Your business has established regular information security awareness training for all staff. Your business ensures that employees and contractors are aware of and fulfil their information security responsibilities.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should brief all staff on their security responsibilities, including the appropriate use of business systems and ICT equipment. You should also train your staff to recognise common threats such as phishing emails and malware infection and how to recognise and report data security breaches.

You should ensure that staff with specific security responsibilities or with privileged access to business systems are adequately trained and qualified as appropriate.

You should schedule training to take place on or shortly after appointment with updates at regular intervals thereafter or when required. You should also reinforce training using other methods including intranet articles, circulars, team briefings and posters.

Well-designed security measures will not work if staff do not know about or follow business policies and procedures. You should make policies and procedures available to all staff using staff intranet pages, policy libraries or through leaflets and posters.

It is good practice to circulate bulletins or newsletters to help disseminate and inform staff of new policies and subsequent updates when required.

Areas for focus and suggested actions

Staff with specific security responsibilities or with privileged access to business systems should be adequately trained and qualified as appropriate.

You should:

- Brief all staff on their security responsibilities, including the appropriate use of business systems and ICT equipment.
- Train your staff to recognise common threats such as phishing emails and malware infection and how to recognise and report data security breaches.
- Ensure staff are trained on or shortly after appointment with updates at regular intervals thereafter or when required.
- Reinforce training using other methods including intranet articles, circulars, team briefings and posters.

Guidance

User education and awareness, in 10 steps to cyber security, National Cyber Security Centre **www.www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness**

Training checklist for small to medium sized organisations, ICO **www./ico.org.uk/media/for-organisations/documents/1606/training-checklist.pdf**

Step 3 of 4: Physical security

3.1 Secure areas

Your business has established entry controls to restrict access to premises and equipment on a need-to-know basis. Your business prevents unauthorised physical access, damage and interference to personal data.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should implement entry controls including doors and locks and whether premises are protected by alarms, security lighting or CCTV. You should also implement how you control access within premises and supervise visitors. Servers should be located in a separate room and protected by additional controls.

Areas for focus and suggested actions

It is important to establish entry controls to restrict access to your premises and equipment and prevent unauthorised physical access, damage and interference to personal data.

You should:

- Restrict access to a 'need-to-know' basis only.
- Implement appropriate entry controls including doors and locks, alarms, security lighting or CCTV.
- Control access within your premises and have effective visitor procedures including measures such as signing-in protocols, name badges and escorted access.
- Consider ID badge systems for staff.
- Locate equipment or storage facilities housing more sensitive personal data (including servers) in a separate room, protected by additional controls.

Guidance

Information security, ICO Guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/**

Physical security, Get safe online website **www.getsafeonline.org/hardware-and-devices/physical-security/**

3.2 Secure storage

Your business has established secure storage arrangements to protect records and equipment. Your business prevents loss, damage, theft or compromise of personal data.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

All your staff should lock away paper records and mobile computing devices when not in use ('clear desk and equipment'). Also, you should encourage staff to promptly collect documents from printers, fax machines and photocopiers and you should switch devices off outside business hours. Ideally, you should implement secure printing.

Areas for focus and suggested actions

All your staff should lock away paper records and mobile computing devices when not in use ('clear desk and equipment').

You should:

- Implement a 'clear desk' policy and introduce compliance checking mechanisms within your organisation.
- Ensure that there are adequate secure storage facilities provided to store mobile equipment and hardware, as well as paper records.
- Encourage staff to promptly collect documents from printers, fax machines and photocopiers, and ensure these devices are switched off outside business hours.

Guidance

Information Security, ICO Guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/**

3.3 Secure Disposal

Your business has established a process to securely dispose of records and equipment when no longer required.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

All your staff should securely dispose of paper records by shredding. If you use a provider to erase data and dispose of or recycle your computers, make sure they do it adequately. You may be held responsible if personal data collected by you is extracted from your old equipment if it is resold.

Areas for focus and suggested actions

It is important that all your staff dispose of paper records and equipment storing personal data securely.

You should:

- Identify and store paper records that contain personal data that require secure disposal through the use of confidential waste bins (which are locked/secure when not in use).
- Store equipment or hardware that contained personal data in a secure location whilst awaiting destruction/disposal.
- Securely dispose of paper records by shredding - ideally a cross cut shredder should be used.
- If you use a third party provider to shred paper records, erase data or dispose of/recycle your equipment or hardware, make sure they do it adequately and you have appropriate assurances in place to confirm compliance.
- Keep a log of all equipment and confidential waste that is sent for disposal or destruction and, where possible, retain certificates of destruction.

Guidance

IT asset disposal, ICO **www.ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf**

Safe computer disposal, Get safe online website **www.getsafeonline.org/protecting-your-computer/safe-computer-disposal/**

Step 4 of 4: Computer and network security

4.1 Home and mobile working procedures

Your business has established a mobile working policy. Your business ensures the security of mobile working and the use of mobile computing devices.

- ○ Not yet implemented or planned
- ○ Partially implemented or planned
- ○ Successfully implemented
- ○ Not applicable

Mobile working can involve the storage and transit of personal data outside the secure boundaries of your business. However, mobile computing devices (for example, laptops, notebooks, tablets and smartphones) are vulnerable to theft and loss and there are confidentiality risks when using devices in public places.

You should assess the risks of mobile working (including remote working where mobile devices can connect to the corporate network) and devise a policy that sets out rules for authorising and managing mobile working.

Areas for focus and suggested actions

Mobile working can involve the storage and transit of personal data outside the secure boundaries of your business. However, mobile computing devices (for example, laptops, notebooks and smartphones) are vulnerable to theft and loss, and there are confidentiality risks when using devices in public places. Therefore, you should:

- Assess the risks of mobile working (including remote working where mobile devices can connect to the corporate network).
- Establish a mobile working policy (based on the outcomes of the risk assessment) to assist in ensuring the security of mobile working and the use of mobile computing devices.
- Implement a process that sets out procedures to follow for authorising and managing mobile working.
- Keep a log of all mobile devices used in your organisation and who they are allocated to.

Guidance

Home and mobile working, in 10 steps to cyber security, National Cyber Security Centre **www.ncsc.gov.uk/guidance/10-steps-home-and-mobile-working**

Bring your own device (BYOD), ICO **www.ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf**

4.2 Secure configuration

Your business has established a process to configure new and existing hardware to reduce vulnerabilities and provide only the functionality and services required.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

The default installation of ICT equipment can include vulnerabilities such as unnecessary guest or administrative accounts, default passwords that are well known to attackers and pre-installed but unnecessary software. These vulnerabilities can provide attackers with opportunities to gain unauthorised access to personal data held in business systems.

You should securely configure (or 'harden') ICT equipment on installation. Maintaining an inventory of ICT equipment will help you to identify and remove unnecessary or unauthorised hardware and software.

Areas for focus and suggested actions

The default installation of ICT equipment can include vulnerabilities such as unnecessary guest or administrative accounts, default passwords that are well known to attackers and pre-installed but unnecessary software. These vulnerabilities can provide attackers with opportunities to gain unauthorised access to personal data held in business systems. Therefore you should:

- Establish a process to configure new and existing hardware to reduce vulnerabilities and provide only the functionality and services required.
- Maintain an up-to-date inventory of ICT equipment.

Guidance

Secure configuration, in 10 steps to cyber security, National Cyber Security Centre **www.ncsc.gov.uk/guidance/10-steps-secure-configuration**

A practical guide to IT security, ICO **www.ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf**

Unnecessary services and default credentials, in protecting personal data in online services, ICO **www.ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf**

4.3 Removable media

Your business has established controls to manage the use of removable media. Your business prevents unauthorised disclosure, modification, removal or destruction of personal data stored on media.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Removable media (for example, CD/DVDs, USB drives, smartphones) is highly vulnerable to theft or loss and uncontrolled use can lead to data breaches.

Where there is a business need to store personal data on removable media, you should implement a software solution that can set permissions or restrictions for individual devices as well as entire classes of devices. Personal data should be minimised and encrypted.

Areas for focus suggested actions

Removable media (for example, CD/DVDs, USB drives, smartphones) is highly vulnerable to theft or loss, and uncontrolled use can lead to data leakage.

You should:

- Minimise and encrypt personal data stored on mobile devices.
- Protect personal data in transit by a secure remote working solution such as a Virtual Private Network.
- Implement access controls or software solutions to mobile devices such as pin controlled access, data/disc encryption and limited systems access.

Guidance

Removable media controls, in 10 steps to cyber security, National Cyber Security Centre **www.ncsc.gov.uk/guidance/10-steps-removable-media-controls**

4.4 User access controls

Your business has established a process to assign user accounts to authorised individuals and to manage user accounts effectively to provide the minimum access to information. Your business limits access to personal data held in information systems.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Access to systems holding personal data should be authorised by management and user permissions restricted to the absolute minimum (or 'least privilege'). You should assign each user their own username and password to ensure accountability.

Areas for focus and suggested actions

It is important that your business limits access to personal data held in information systems.

You should:

- Implement a process to ensure that access to systems holding personal data is authorised by management.
- Restrict user permissions to the absolute minimum (or 'least privilege').
- Assign each user with their own username and password to ensure accountability.
- Implement role based user profiles and access levels to ensure that access to systems is only given to those roles that require it in order to complete their work.
- Review all network and application user access lists at least annually.
- Ensure you have robust starter, mover and leaver processes in place to avoid the risk of unauthorised access or the accrual of unnecessary access levels.

Guidance

Managing user privileges, in 10 steps to cyber security, National Cyber Security Centre **www.ncsc.gov.uk/guidance/10-steps-managing-user-privileges**

Information access management, Get safe online website **www.getsafeonline.org/businesses/information-access-management/**

Password storage, in protecting personal data in online services, ICO **www.ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf**

4.5 System Password Security

Your business has established appropriate password security procedures and 'rules' for information systems and has a process in place to detect any unauthorised access or anomalous use.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Users' access credentials (e.g. a username and password or passphrase) are particularly valuable to attackers. A 'brute force' password attack is a common threat so you need to enforce strong passwords, regular password changes and limit the number of failed login attempts.

You should enable and actively encourage your users to choose a strong password. You can increase the strength and complexity of a password by:

- Creating a long password or passphrase using a wide range of characters, such as a mix of uppercase letters, lowercase letters, numbers, punctuation marks and other symbols.
- Avoiding the use of dictionary words where possible.
- Avoiding simple substitutions such as 'p4$$w0rd'.
- Avoiding the use of patterns derived from the physical keyboard layout (e.g. 'qwerty' or '1qaz2wsx').

You should also monitor user activity to detect any anomalous use.

Having multiple passwords for different systems can be difficult for staff to remember, however, it is important that passwords are not written down or recorded in accessible locations or systems logs.

You should promptly disable passwords when a user changes duties or leaves the business.

Areas for focus and suggested actions

Users' access credentials (e.g. a username and password or passphrase) are particularly valuable to attackers. A 'brute force' password attack is a common threat so you need to:

- Install malware protection software to regularly scan your computer network in order to detect and prevent threats.
- Make sure the software is kept up-to-date.
- Educate users about common threats.

Guidance

Malware prevention, in 10 steps to cyber security, National Cyber Security Centre **www.ncsc.gov.uk/guidance/10-steps-malware-prevention**

Viruses and spyware, Get safe online website **www.getsafeonline.org/protecting-yourself/viruses-and-spyware/**

4.7 Backup and restoration

Your business has established a process to routinely back-up electronic information to help restore information in the event of disaster. Your business ensures protection against the loss of personal data.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should take regular back-ups to help restore personal data in the event of disaster or hardware failure. The extent and frequency of back-ups should reflect the sensitivity and confidentiality of the personal data and its criticality to the continued operation of the business.

Ideally, you should keep back-ups in a secure location away from the business premises and regularly test the restoration of personal data to check the effectiveness of the back-up process.

Areas for focus and suggested actions

You should take regular back-ups to help restore personal data in the event of disaster or hardware failure. The extent and frequency of back-ups should reflect the sensitivity and confidentiality of the personal data, and its criticality to the continued operation of the business. You should:

- Establish a process to routinely back-up electronic information to help restore information in the event of disaster.
- Ensure back-ups are kept in a secure location away from the business premises.
- Test the restoration of personal data regularly to check the effectiveness of the back-up process.

Guidance

Backups, Get Safe online website **www.getsafeonline.org/protecting-your-computer/Backups/**

4.8 Monitoring

Your business has established a process to log and monitor user and system activity to identify and help prevent data breaches. Your business records events and generates evidence.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Monitoring and logging can help your business to detect and respond to external threats and any inappropriate use of information assets by staff.

You should continuously monitor inbound and outbound network traffic to identify unusual activity (e.g. large transfers of personal data) or trends that could indicate an attack.

Business systems should be capable of logging user access to systems holding personal data in support of access control policy monitoring and investigations.

Monitoring and logging must comply with any legal or regulatory constraints, including the DPA e.g. you should make staff aware of any monitoring.

Areas for focus and suggested actions

Monitoring and logging can help your business to detect and respond to external threats and any inappropriate use of information assets by staff.

You should:

- Establish a process to log and monitor user and system activity to identify and help prevent data breaches.
- Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate an attack.
- Implement a mechanism to log user access to systems holding personal data in support of an access control policy.
- Ensure all monitoring and logging complies with any legal or regulatory constraints.
- Make staff aware of any monitoring you undertake.

Guidance

Monitoring, 10 steps to cyber security, National Cyber Security Centre **www.ncsc.gov.uk/guidance/10-steps-monitoring**

Employment code of practice, ICO **www.ico.org.uk/media/for-organisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf**

4.9 Patch management

Your business has established a process to ensure software is kept up-to-date and the latest security patches are applied. Your business prevents the exploitation of technical vulnerabilities.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Most popular software products contain technical vulnerabilities that can be exploited by attackers to gain unauthorised access to personal data held in your systems.

You should use the latest versions of operating systems, web browsers and applications, and ensure these are updated regularly to help prevent the exploitation of unpatched vulnerabilities.

Areas for focus and suggested actions

Most popular software products contain technical vulnerabilities that can be exploited by attackers to gain unauthorised access to personal data held in your systems.

You should:

- Establish a process to log and monitor user and system activity to identify and help prevent data breaches.
- Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate an attack.
- Implement a mechanism to log user access to systems holding personal data in support of an access control policy.
- Ensure all monitoring and logging complies with any legal or regulatory constraints.
- Make staff aware of any monitoring you undertake.

Guidance

Software security updates in protecting personal data in online services, ICO **www.ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf**

4.10 Boundary firewalls

Your business has established boundary firewalls to protect computers from external attack and exploitation. Your business ensures the protection of personal data in networks.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Attackers can gain unauthorised access to personal data if you do not protect the boundary between your computer network and the internet.

You should install a firewall to monitor and restrict network traffic based on an agreed set of rules. A well configured firewall is your first line of defence against external attack and can help to prevent data breaches, for example, by blocking malware or hacking attempts.

You should also minimise the impact of data breaches by segmenting and limiting access to network components that contain personal data e.g. your web server should be separate from your main file server. If your website is compromised then the attacker will not have direct access to your central data store.

Areas for focus and suggested actions

Attackers can gain unauthorised access to personal data if you do not protect the boundary between your computer network and the internet. A well configured firewall is your first line of defence against external attack and can help to prevent data breaches e.g. by blocking malware or hacking attempts. Therefore you should:

- Install a firewall to monitor and restrict network traffic based on an agreed set of rules.

- Minimise the impact of data breaches by segmenting and limiting access to network components that contain personal data e.g. your web server should be separate from your main file server. If your website is compromised then the attacker will not have direct access to your central data store.

Guidance

Network security, in 10 steps to cyber security, National Cyber Security Centre **www.ncsc.gov.uk/guidance/10-steps-network-security**

Inappropriate locations for processing personal data, in protecting personal data in online services, ICO **www.ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf**

GDPR checklist for direct marketing

Notes

GDPR checklist for direct marketing

This GDPR checklist has been created by the ICO (Information Commissioners Office) to help prepare businesses for the new data protection laws due to come in to force on 25th May 2018. We believe this to be a useful tool for our members and non-members and for all small to medium sized organisations from the private, public and third sectors.

Effective information handling makes good business sense. You will enhance your business's reputation, increase customer and employee confidence and, by making sure personal information is accurate, relevant and safe, save both time and money.

Checklist for businesses involved in direct marketing.

The new GDPR laws covers companies involved in direct marketing. The checklist is designed to enable you to assess in line with the Privacy and Electronic Communications Regulation (PECR) and covers all aspects including consent and bought-in marketing lists, telephone, email, text and postal marketing.

It is important to note that direct marketing is the promotion of aims and ideals as well as the sale of products and services.

If you would like to complete this online checklist please visit **www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/direct-marketing/**

On completion, a short report will be created suggesting practical actions you can take to ensure you are compliant with the GDPR. It will also provide links to additional guidance that will help ensure your business meets the new data protection laws.

Do you process personal data as a data controller or a data processor?

Before you undertake the GDPR checklist you should first determine whether your role in the process is as a data controller or as a data processor.

The definition of the two terms are:

Data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is, or will be processed.

Data processor is responsible for processing personal data on behalf of a controller. If you are processor, the GDPR places specific legal obligations on you. For example, you will be required to maintain records of personal data and processing activities and you will have legal liability if you are responsible for a breach

In some instances, an organisation will process personal information as both a data controller and a data processor. When this is the case, the ICO would advise that both assessments for a controller and processor are completed. Access to both checklists can be found here:

www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

Step 1: Consent

Your business has obtained the necessary consent from individuals for marketing in compliance with the DPA and PECR (Privacy and Electronic Communications Regulations).

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

In many cases you must obtain prior 'opt-in' consent to send marketing communications and it is always good practice to use opt-in boxes when collecting contact details for marketing purposes.

You should tell people what methods of marketing communication you are going to use, e.g. email, text, phone, automated call, post.

You should ask for consent to pass contact details to third parties for marketing and name or describe those third parties with enough detail to give people an informed choice over marketing.

You should record when and how you obtained consent and exactly what it covers to ensure you do not inadvertently contact people against their wishes. You can keep a 'suppression list' of people who don't want to receive marketing.

Areas for focus and suggested actions

In many cases you must obtain prior 'opt-in' consent to send marketing communications and it is always good practice to use opt-in boxes when collecting contact details for marketing purposes.

You should:

- Specify methods of marketing communication (e.g. by email, text, phone, automated call, post).
- Ask for consent to pass contact details to third parties for marketing, and name or describe those third parties.
- Record when and how you obtained consent and exactly what it covers to ensure you do not inadvertently contact people against their wishes.

Guidance

Consent, in ICO direct marketing guidance **www.ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf**

The DMA Code, Direct Marketing Association website **www.dmcommission.com/the-dma-code/**

What counts as consent in Key definitions, ICO Guide to PECR **www.ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/**

Step 2: Bought-in lists

Your business has sought assurances about the origins and accuracy of any bought-in lists.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Neither the DPA or PECR ban the use of bought-in marketing lists but you should take steps to ensure the list was compiled fairly and accurately, reflects people's wishes and is reasonably up to date.

You should check when and how consent was obtained and what it covers to ensure you do not inadvertently contact people against their wishes.

You should always screen bought-in lists against the TPS when making live marketing calls.

You should avoid using bought-in lists for emails, texts or automated calls unless you have proof of 'opt-in' consent within the last six months, which specifically names or describes your business.

You should tell people where you got their details if asked.

Areas for focus and suggested actions

Neither the DPA or PECR ban the use of bought-in marketing lists but you should take steps to ensure the list was compiled fairly and accurately reflects people's wishes:

You should:

- Check when and how consent was obtained and what it covers to ensure you do not inadvertently contact people against their wishes.
- Always screen bought-in lists against the TPS when making live marketing calls.
- Avoid using bought-in lists for emails, texts or automated calls unless you have proof of 'opt-in' consent within the last six months, which specifically names or describes your business.
- Tell people where you got their details if asked.

Guidance

Direct marketing checklist, ICO **www.ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf**

Buying a marketing list, in ICO direct marketing guidance **www.ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf**

The DMA Code, Direct Marketing Association website **www.dmcommission.com/the-dma-code/**

Using marketing lists, in ICO Guide to PECR **www.dmcommission.com/the-dma-code/**

Step 3: Telephone marketing

Your business identifies itself when making marketing calls and makes them only in accordance with the express wishes of recipients in compliance with PECR.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You must screen live marketing calls against the TPS. The only exception to this rule is where people have told you that, for the time being, they do not object to receiving such calls.

It is good practice to maintain your own 'do not call' list to screen live marketing calls.

You must obtain prior 'opt-in' consent to make automated marketing calls. There is no exception to this rule.

You must identify your business and provide a valid business address or Freephone number. You can do so in the content of an automated call recording or when asked during a live call.

Areas for focus and suggested actions

It is important that your business identifies itself when making marketing calls and makes them only in accordance with the express wishes of recipients in compliance with PECR.

You should:

- Screen live marketing calls against the Telephone Preference Service (TPS). The only exception to this rule is where people have told you that, for the time being, they do not object to receiving such calls.
- Maintain your own 'do not call' list to screen live marketing calls.
- Obtain prior 'opt-in' consent to make automated marketing calls. There is no exception to this rule.
- Identify your business and provide a valid business address or Freephone number. You can do so in the content of an automated call recording or when asked during a live call.

Guidance

Direct marketing checklist, ICO **www.ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf**

Marketing calls, in ICO direct marketing guidance **www.ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf**

The DMA Code, Direct Marketing Association website **www.dmcommission.com/the-dma-code/**

Telephone marketing, in ICO Guide to PECR **www.ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/telephone-marketing/**

Step 4: Electronic marketing

Your business identifies itself when sending electronic marketing messages and ensures the initial and ongoing permission of recipients in compliance with PECR.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You must obtain prior 'opt-in' consent to send electronic marketing messages by email, text, picture or video messaging. The only exception to this rule is where you intend to contact previous customers about similar products or services provided by your business and they were offered an 'opt-out' when you first collected their contact details.

You must identify your business and provide an easy means to opt-out of receiving further electronic marketing with every message. You should therefore provide a valid email address or short code number for texts (as long as this does not incur premium rate charges). It is good practice to provide a link to your website for further contact details.

It is good practice to maintain your own 'do not contact' list to screen electronic marketing messages.

Areas for focus and suggested actions

You must obtain prior 'opt-in' consent to send electronic marketing messages by email, text, picture or video messaging. The only exception to this rule is where you intend to contact previous customers about similar products or services provided by your business and they were offered an 'opt-out' when you first collected their contact details .

You should:

- Identify your business and provide an easy means to opt-out of receiving further electronic marketing with every message.
- Provide a valid email address or short code number for texts (as long as this does not incur premium rate charges).
- Provide a link to your website where further contact details can be found.
- Maintain your own 'do not contact' list to screen electronic marketing messages.

Guidance

Direct marketing checklist, ICO **www.ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf**

Marketing texts and emails, in ICO direct marketing guidance **www.ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf**

The DMA Code, Direct Marketing Association website **www.dmcommission.com/the-dma-code/**

Electronic mail marketing, in ICO Guide to PECR **www.ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/**

Electronic mail marketing, ICO marketing sector page **www.ico.org.uk/for-organisations/marketing/**

Step 5: Postal marketing

Your business only sends marketing mail to named individuals who have not objected to receiving mailings in compliance with the DPA.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Section 11 of the DPA gives individuals the right to issue your business with a written notice that their details should not be used for marketing purposes. Your business must comply with this notice. It is good practice to acknowledge the notice and confirm the marketing will stop.

It is good practice to screen marketing mailings against the Mailing Preference Service (MPS) and you should also maintain your own 'do not contact' list to screen those who have notified you directly that they object to the receipt of marketing mailings.

Areas for focus and suggested actions

Section 11 of the DPA gives individuals the right to issue your business with a written notice that their details should not be used for marketing purposes. On receipt your business must comply with this notice.

You should:

- Acknowledge the notice and confirm the marketing will stop.
- Screen marketing mailings against the Mailing Preference Service (MPS).
- Maintain your own 'do not contact' list to screen those who have notified you directly that they object to the receipt of marketing mailings.

Guidance

Preventing direct marketing, in ICO Guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/preventing-direct-marketing/**

Direct marketing checklist, ICO.

Marketing mail, in ICO direct marketing guidance **www.ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf**

Postal marketing, ICO marketing sector page **www.ico.org.uk/for-organisations/marketing/**

GDPR checklist for records management

Notes

GDPR checklist for records management

This GDPR checklist has been created by the ICO (Information Commissioners Office) to help prepare businesses for the new data protection laws due to come in to force on 25th May 2018. We believe this to be a useful tool for our members and non-members and for all small to medium sized organisations from the private, public and third sectors.

Effective information handling makes good business sense. You will enhance your business's reputation, increase customer and employee confidence and, by making sure personal information is accurate, relevant and safe, save both time and money.

Checklist for businesses involved in records management.

GDPR covers record management as part of the new data protection laws. This checklist enables you to assess your business in the specific area of records management policy and the associated risks to people's personal information. The assessment includes record creation, storage and disposal, access, tracking and off-site storage.

If you would like to complete this online checklist please visit **www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/records-management/**

On completion, a short report will be created suggesting practical actions you can take to ensure you are compliant with the GDPR. It will also provide links to additional guidance that will help ensure your business meets the new data protection laws.

Do you process personal data as a data controller or a data processor?

Before you undertake the GDPR checklist you should first determine whether your role in the process is as a data controller or as a data processor.

The definition of the two terms are:

Data **controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is or will be processed.

Data **processor** is responsible for processing personal data on behalf of a controller. If you are processor, the GDPR places specific legal obligations on you. For example, you will be required to maintain records of personal data and processing activities and you will have legal liability if you are responsible for a breach.

In some instances, an organisation will process personal information as both a data controller and a data processor. When this is the case, the ICO would advise that both assessments for a controller and processor are completed. Access to both checklists can be found here:

www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

Step 1 of 4: Management and organisational records management

1.1 Records management organisation

Your business has defined and allocated records management responsibilities.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should assign lead responsibility for records management within the organisation at a level of seniority high enough to be able to affect change to policy, process and culture.

Where resources are available, you should nominate an appropriately skilled records management lead to coordinate the management of records within the business. This may be combined with other roles within the organisation.

Areas for focus and suggested actions

You should assign lead responsibility for records management within the organisation at a level of seniority high enough to be able to affect change to policy, process and culture.

You should:

- Nominate an appropriately skilled records management lead to coordinate the management of records within your business.
- Ensure they have the necessary authority and resources to fulfil this responsibility effectively.
- For larger organisations, appoint 'owners' with day-to-day responsibility for the security, use, accuracy and retention of manual and electronic records.

Guidance

Organisational arrangements to support records management, in National Archives records management guide 2 **www.nationalarchives.gov.uk/documents/information-management/rm-code-guide2.pdf**

1.2 Records management policy

Your business has approved and published an appropriate records management policy. This is subject to a regular review process.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

A policy will enable you to address how records are used within your organisation in a consistent manner. This can be part of a general policy or a standalone policy statement that is supported by specific records management procedures such as storage and maintenance of records or disposal of records.

The policy should clearly set out your business's approach to records management and as a minimum should address the organisation's overall commitment, the role of records management, references to related policies and documents, staff roles and responsibilities and monitoring of compliance.

The National Archives has developed comprehensive guidance on how to create an effective records management policy.

Areas for focus and suggested actions

A policy will enable you to address how records are used within your organisation in a consistent manner. This can be part of a general policy or a standalone policy statement that is supported by specific records management procedures such as storage and maintenance of records or disposal of records.

You should:

- Clearly set out in policy your business's approach to records management together with responsibilities for implementing the policy and monitoring compliance.
- Ensure the policy is approved by management, published and communicated to all staff.
- Review and update the policy at planned intervals or when required to ensure it remains relevant.

The National Archive has developed comprehensive guidance on how to create an effective records management policy.

Guidance

Records management policy, National Archives **www.nationalarchives.gov.uk/documents/information-management/rm-code-guide3.pdf**

1.3 Records management risk

Your business has identified records management risks as part of a wider information risk management process.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should carry out regular exercises to identify, assess and manage records management risks. This process simply seeks to identify what might go wrong with a process and why. Measures can then be put in place to mitigate these risks.

Where a corporate risk register is already in place this can be used to record risks to records management function. These might include records not being updated, not being destroyed in a timely manner or not being held securely.

Suggested actions

You should carry out regular exercises to identify, assess and manage records management risks. This process simply seeks to identify what might go wrong with a process and why. You can then put measures in place to mitigate these risks.

You should:

- Undertake a risk assessment of all records held within your organisation.
- Where a corporate risk register is already in place, record risks to records management functions (these might include records not being updated, not being destroyed in a timely manner or not being held securely).

Guidance

Inclusion of records management and information management in the corporate risk management framework, in National Archives records management guide 2 **www.nationalarchives.gov.uk/documents/information-management/rm-code-guide2.pdf**

Assessing and Managing Risk, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/managing-risk/assessing-managing-risk/**

1.4 Records management training

Your business incorporates records management (RM) within a formal training programme. This comprises mandatory RM induction training with regular refresher material and specialist training for those with specific RM functions.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should brief all staff on their responsibilities for the creation, use, maintenance and eventual destruction of records on or shortly after appointment with regular updates to maintain levels of awareness. Awareness materials might include posters, office wide emails, intranet updates, records management content in newsletters.

Staff with specific records management responsibilities such as management of disposal schedules, monitoring of data quality or oversight of records management practice should receive appropriate training in order to allow them to carry out their role effectively.

Areas for focus and suggested actions

You should brief all staff on their responsibilities for the creation, use, maintenance and eventual destruction of records.

You should:

- Ensure your business has incorporated records management (RM) within a formal training programme that comprises mandatory RM induction training and delivery of regular refresher material for all staff.
- Provide specialist training to those with specific RM functions.
- Promote records management awareness generally amongst all staff through various promotional materials such as posters, newsletters and intranet articles.

Guidance

Guide to outsourcing for SMEs, ICO **www.ico.org.uk/media/for-organisations/documents/1585/outsourcing_guide_for_smes.pdf**

Training checklist for SMEs, ICO **www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/TRAININGCHECKLIST_V1_WEB_VERSION.ashxf**

1.5 Outsourcing

Your business has established written agreements with third party service providers that include appropriate information security conditions. Your business ensures the protection of personal data that is accessed by suppliers and providers.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Many small businesses outsource some or all of their data processing requirements to hosted (including cloud based) services e.g. for archiving purposes, confidential waste disposal or IT network services. You should be satisfied that these 'data processors' will treat your information securely as your business will be held responsible under the DPA for what they do with the personal data.

You must choose a provider that gives sufficient guarantees about its security measures e.g. you might review copies of any security assessments and, where appropriate, visit their premises to make sure appropriate security arrangements are in place.

You must also have a written contract setting out what the provider is allowed to do with the personal data and requiring them to take the same security measures you would have to take to comply with the DPA.

Areas for focus and suggested actions

If you outsource the processing of personal data you may still remain responsible for the data under the DPA and therefore you should:

- Choose an organisation that provides sufficient guarantees about how it will protect the data.
- Ensure written and enforceable contracts are in place setting out information security conditions.
- Consider whether outsourcing involves the transfer of data overseas (which could include hosted services or cloud computing solutions) and ensure the recipient will provide adequate protection.

Guidance

Guide to outsourcing for SMEs, ICO **www.ico.org.uk/media/for-organisations/documents/1585/outsourcing_guide_for_smes.pdf**

Information security, in ICO guide to data protection **www.ico.org.uk/for_organisations/data_protection/the_guide/principle_7**

Guidance on the use of cloud computing, ICO **www.ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf**

Model contract clauses – International transfers of personal data, ICO **www.ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf**

Model contracts for the transfer of personal data to third countries, European Commission **www.ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm**

1.6 Monitoring and reporting

Your business carries out periodic checks on records security and there is monitoring of compliance with records management procedures. The outcomes of any records security checks or compliance monitoring is measured against key performance indicators to provide strategic oversight to those with overall responsibility for RM.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should develop ways of checking staff compliance to ensure policies and procedures are adhered to e.g. after hours desk sweeps to ensure compliance with clear desk policy, checks of disposal procedures to ensure that confidential waste is being disposed of correctly.

Performance measures might include progress against a records management action plan, archive retrieval rates measured against a service level agreement (SLA), progress regarding deletion of records against requirements of a retention schedule or data quality and accuracy. Reports on performance to KPIs should be reported periodically to management to provide assurances on compliance.

Areas for focus and suggested actions

You should develop ways of checking compliance to ensure policies and procedures are adhered to.

You should:

- Undertake periodic checks on records security and monitor compliance with records management procedures.
- Measure the outcomes of any records security checks or compliance monitoring against key performance indicators to provide strategic oversight to those with overall responsibility for RM.

Step 2 of 4: Records creation and maintenance

2.1 Record creation

Your business has minimum standards for creation of paper or electronic records and has established processes to ensure that there is a legitimate purpose for using personal data prior to collecting it.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should ensure procedures and guidelines for referencing, titling and indexing new records are in place to control access to those records and allow for efficient management, retrieval and disposal.

If the collection of data is in your organisation's legitimate interests, and is fair and lawful, you will most likely comply with the DPA.

Although emails are often perceived differently to other records, they still contain information which has a wider business purpose as well as personal or sensitive personal data, so you should managed them in a consistent way.

Suggested actions

You should ensure procedures and guidelines for referencing, titling and indexing new records are in place in order to provide for controlled access to such records and allow for efficient management, retrieval and disposal.

You should:

- Ensure you have minimum standards for creation of paper or electronic records in place and have processes that establish that there is a legitimate purpose for using personal data prior to collecting it (which includes email).
- Establish procedures and guidelines for staff to ensure new records are titled and indexed in a way that allows efficient management, retrieval and disposal.

- Where applicable, ensure you have some form of security classification or marking protocols in place, such as the Government protective marking scheme, to identify records that contain more sensitive information.

Guidance

Keeping records to meet corporate requirements, National Archives **www.nationalarchives.gov.uk/documents/information-management/rm-code-guide4.pdf**

Processing personal data fairly and lawfully, in ICO Guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/**

Managing digital records without an electronic record management system, National Archives **www.nationalarchives.gov.uk/documents/information-management/managing-electronic-records-without-an-erms-publication-edition.pdf**

Managing emails, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/policy-process/managing-email/**

2.2 Records inventory

Your business has identified manual and electronic record keeping systems throughout the organisation and actively maintains a centralised record of those systems.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

In order to ensure that personal data is managed effectively and securely it is necessary for you to know what information you hold and how. As such it may be necessary to carry out an 'information audit' or 'records survey' to identify records and data sets held by the organisation.

This process will help in determining which business functions create certain records, which records are vital to the functioning of the business, where they are kept, how long they are kept for and who needs to use them now and in the future.

Once this information is gathered it may allow for the development of retention and disposal schedules, improved security practices, and the development of disaster recovery processes.

Areas for focus and suggested actions

In order to ensure that personal data is managed effectively and securely it is necessary for you to know what you hold and how.

You should:

- Carry out an 'information audit' or 'records survey' to identify records and data sets held by the organisation.
- Create a central log or record of which business functions create certain records, which records are vital to the functioning of the business, where they are kept, how long they are kept for and who needs to use them now and in the future.

Guidance

Undertaking a records survey, JISC **www.jiscinfonet.ac.uk/infokits/records-management/semi-active-use/record-survey/**

Find out what information you have, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/find-out-what-information-you-have/**

2.3 Information standards

Your business has processes in place to ensure that personal data that is collected is accurate, adequate, relevant and not excessive. Routine weeding is also carried out to remove any personal data or records that are no longer relevant or out of date.

- ○ Not yet implemented or planned
- ○ Partially implemented or planned
- ○ Successfully implemented
- ○ Not applicable

The DPA requires that personal data is accurate and up-to-date. What is considered to fall under these categories will change over time and as an organisation's business needs change. You should have processes in place to ensure that personal data which is inaccurate or is out of date is removed from records on a regular basis.

You should have a process in place to ensure that you take reasonable steps to ensure the accuracy of personal data collected and to deal with challenges to the accuracy of personal data from individuals about whom information is recorded over time. This should allow for the personal data to be amended, removed or clarified where appropriate.

The DPA says that personal data should be adequate, relevant and not excessive. If you do not make decisions regarding what personal data you should hold for your business purposes then you are at risk of collecting excessive data and infringing the privacy of an individual, or you may hold too little to facilitate effective decision making about those individuals. Again what is adequate, relevant and not excessive will change with business need.

Areas for focus and suggested actions

The DPA requires that personal data is accurate and up-to-date. What is considered to fall under these categories will change over time and as an organisation's business needs change. You should therefore have processes in place to ensure that personal data which is inaccurate or is out of date is removed from records on a regular basis. In addition, the DPA says that personal data should be adequate, relevant and not excessive. If you do not make decisions regarding what personal data you should hold for your business purposes then you are at risk of collecting excessive data and infringing the privacy of an individual or you may hold too little to facilitate effective decision making regarding individuals.

You should therefore:

- Ensure a process is in place to guarantee appropriate steps are taken to confirm the accuracy of personal data that is newly collected, or that has been recorded and retained over a period of time.

- Establish initial and then periodic reviews to check that data collected is not excessive for the purpose/processing requirements.
- Where information is identified as out of date, regular records weeding should take place to remove inaccurate data.

Guidance

The amount of personal data you may hold, in ICO guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/**

Keeping personal data accurate and up to date, in ICO guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/**

Retaining personal data, in ICO guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/**

Step 3 of 4: Tracking and offsite storage

3.1 Tracking and offsite storage of paper records

Your business has tracking mechanisms to record the movement of manual records and ensure their security between office and storage areas and also in instances where records are taken offsite.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

In many circumstances employees will be required to take paper records offsite in order to work remotely, e.g. to visit service users or to attend court hearings. Equally you may wish to store archived records offsite due to limitations on space within your offices. When doing so, you should have appropriate procedures in place to ensure that your business knows what records are offsite and who is holding them so you can recover them if necessary or destroy them when they reach the end of their retention period.

When transferring data offsite, it should be minimised, use an appropriate form of transport, e.g. secure courier for sensitive personal data, log the transfer in and out where appropriate and put checks in place to ensure that data is received. Security measures which you could use include lockable containers, tamper evident packaging, and removal from public view and accessibility.

Areas for focus and suggested actions

Appropriate procedures should be in place to ensure that you know what records are offsite and who is holding them so they can be recovered if necessary or destroyed when they reach the end of their retention period.

You should:

- Implement tracking mechanisms to record the movement and ensure the security of manual records between office and storage areas and also in instances where records are taken offsite.
- Minimise data wherever possible when transferring data offsite.
- Use an appropriate form of transport e.g. secure courier for sensitive personal data.
- Log the transfer in and out where appropriate and put checks in place to ensure that data is received.
- Employ security measures such as lockable containers, tamper evident packaging or removal from public view/accessibility.

Guidance

Tracking Records, National Archives **www.nationalarchives.gov.uk/documents/information-management/tracking-records.pdf**

3.2 Offsite transfer of electronic records

Your business has appropriate measures in place for the transfer of electronic records offsite to protect personal data from loss of theft.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Personal data may be transferred offsite using electronic means such as email or removable media e.g. USB sticks or DVDs. CDs, DVDs, USB drives, smartphones and tablet devices in particular are highly vulnerable to theft or loss.

When transferring data offsite, it should be minimised, you should use an appropriate form of transport e.g. secure courier for sensitive personal data, and you should log the transfer in and out where appropriate and check that data has been received. Security measures which you could use include tamper evident packaging, and storage on encrypted devices.

Where there is a business need to transfer personal data via email or removable media, personal data should be minimised and encrypted. You could use other secure methods such as Secure Transfer Protocols (STP).

Areas for focus and suggested actions

You may transfer personal data offsite using electronic means such as email or removable media e.g. USB sticks or DVDs. CD/DVDs, USB drives, and smartphones in particular are highly vulnerable to theft or loss, and uncontrolled use can lead to data leakage.

You should:

- Always use an appropriate form of transport e.g. secure courier for sensitive personal data when transferring data offsite.
- Minimise data being transported.
- Log the transfer in and out where appropriate and check to ensure that data is received.
- Employ security measures to safeguard the data such as tamper evident packaging, and storage on encrypted devices.

Guidance

Data encryption, Get Safe Online **www.getsafeonline.org/businesses/data-encryption/**

Exporting and transferring electronic data, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/managing-risk/exporting-transferring-electronic-data/**

Step 4 of 4: Security, access and disposal

4.1 Secure storage of records

Your business stores paper and electronic records securely with appropriate environmental controls and higher levels of security around sensitive personal data.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You should use lockable offices, cabinets and drawers to store records, with higher levels of security for records containing sensitive personal data. You should store keys securely and lock records away when staff are absent for extended periods, e.g. overnight. Where screens are left unattended they should be locked to avoid unauthorised access, theft, destruction or alteration of the data displayed with no clear audit trail.

Environmental controls might include waterproofing and drainage to protect against flood risk, fire protection such as use of fire resistant or fire proof materials, fire control systems and heating to protect against damp.

Areas for focus and suggested actions

Paper and electronic records should be stored securely with appropriate environmental controls and higher levels of security around sensitive personal data.

You should:

- Store paper records in lockable offices, cabinets and drawers with higher levels of security around sensitive personal data.

- Ensure keys to such offices, cabinets and drawers are stored securely and records are locked away when staff are absent for extended periods e.g. overnight.
- Consider appropriate environmental controls to protect paper records from threats such as fire or water ingress.
- Implement a clear screen and clear desk policy and culture with regular checks to provide assurances in compliance.

Guidance

Key definitions, in ICO guide to data protection **www.ico.org.uk/for_organisations/data_protection/the_guide/key_definitions**

Information security, in ICO guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/**

Helpful guidance on creating a clear desk policy, Privacy Sense **www.privacysense.net/clear-desk-policy/**

Toolkit for managing paper records, Records Management Society **www.irms.org.uk/resources/information-guides/200-toolkit-for-managing-paper-records_standards**

Protecting archives and manuscripts against disasters, National Archives **www.nationalarchives.gov.uk/documents/information-management/memo6.pdf**

Guidance on the use of cloud computing, ICO **www.ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf**

4.2 Access to paper records

Your business restricts access to records storage areas in order to prevent unauthorised access, damage, theft or loss. Access should be role based in line with the principle of least privilege and checked regularly.

- ○ Not yet implemented or planned
- ○ Partially implemented or planned
- ○ Successfully implemented
- ○ Not applicable

In order to reduce the risk of unauthorised access you should consider who needs access to what personal data in order to fulfil their function. For example, it is likely that only specific members of staff would need access to HR records. In such instances, you should limit access by means of keys, swipe cards, pin codes or other security measures.

Areas for focus and suggested actions

In order to reduce the risk of unauthorised access organisations should consider who needs access to what personal data in order to fulfil their function.

You should:

- Restrict access to records storage areas in order to prevent unauthorised access, damage, theft or loss.

- Implement role based access in line with the principle of least privilege and check access levels regularly.

4.3 Access to electronic records

Your business has a process to assign user accounts to authorised individuals and to remove them when no longer appropriate. Such access should be granted on the basis of least privilege and have appropriate access controls in place.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Access to systems holding personal data should be authorised by management and user permissions restricted to the absolute minimum (known as 'least privilege'). Each user should be assigned their own username and password to ensure accountability.

You should review access permissions periodically to ensure the privileges granted continue to be based on business need and have been correctly authorised. The frequency of review will depend on the level of privilege granted to the user.

A 'brute force' password attack is a common threat so you need to enforce strong passwords, regular password changes, and limit the number of failed login attempts. You should also monitor user activity to detect any anomalous use. Passwords should not be shared unless there is a justified business need and authorisation.

Passwords should be promptly disabled when a user changes duties or leaves the organisation.

Areas for focus and suggested actions

It is important that your business limits access to personal data held in information systems.

You should:

- Implement a process to ensure that access to systems holding personal data is authorised by management.
- Restrict user permissions to the absolute minimum (or 'least privilege').
- Assign each user with their own username and password to ensure accountability.
- Implement role based user profiles and access levels to ensure that access to systems is only given to those roles that require it in order to complete their work.
- Review all network and application user access lists at least annually.
- Ensure you have robust starter, mover and leaver processes in place to avoid the risk of unauthorised access or the accrual of unnecessary access levels.
- Enforce strong passwords are set for both network and systems access.
- Enforce regular password changes and limit the number of failed login attempts.
- Monitor user activity to detect any anomalous use.

Guidance

Information access management, Get Safe Online **www.getsafeonline.org/businesses/information-access-management/**

Managing user privileges, National Cyber Security Centre **www.ncsc.gov.uk/guidance/10-steps-managing-user-privileges**

Password storage, in ICO Protecting personal data in online services guidance **www.ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf**

4.4 Business continuity

Your business has business continuity plans in place. These identify records that are critical to the continued functioning or reconstitution of the organisation in the event of a disaster. Data that is stored electronically is routinely backed-up to help restore information in the event of disaster.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Every organisation will hold data which it cannot function without. You should assess the data held and its criticality to business functions and put plans in place to prepare for serious disruption.

You should take regular backups so that you can restore personal data stored electronically in the event of disaster or hardware failure. The extent and frequency of backups should reflect the sensitivity and confidentiality of the personal data and its criticality to the continued operation of the business. Ideally you should store backups offsite.

Areas for focus and suggested actions

Every organisation will hold data which it cannot function without.

You should:

- Complete an assessment of the data you hold and its criticality to your business functions.
- Ensure business continuity plans are put in place to prepare for serious disruption.
- Take regular backups of systems and data so that you can restore personal data stored electronically in the event of disaster or hardware failure.
- Store backups off site.

Guidance

Business continuity management toolkit, National Archives **www.webarchive.nationalarchives.gov.uk/20121015000000/http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_176447.pdf**

Backups – Information security, Get Safe Online **www.getsafeonline.org/protecting-your-computer/Backups/**

4.5 Disposal of data

Your business has a retention and disposal schedule in place which details how long manual and electronic records will be kept for. Your business has defined confidential waste disposal processes in place to ensure that records are destroyed to an appropriate standard once a disposal decision has been made.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Once you have completed a records survey, you can assign retention periods to records and data sets. Records can then be destroyed once they reach the end of this retention period. You can destroy paper records in a variety of ways including cross cut shredding or incineration. The method of destruction should match the sensitivity of personal data being destroyed and you should carry out checks to ensure that staff are complying with the procedures. Electronic records should also be deleted from systems, however where this is not technically possible, they should be 'put beyond use'. The ICO has published more detailed guidance on deleting personal data.

Where every day confidential waste is awaiting disposal it should be stored securely e.g. in lockable confidential waste bins. Larger storage areas may be required for disposal of large amounts of personal data once it has been weeded from records to be retained.

Areas for focus and suggested actions

Once you have completed a records survey, you can assign retention periods to records and data sets.

You should:

- Have a disposal/retention schedule outlining storage periods for all personal data (this includes manual and electronic records). Regularly review the retention/disposal schedule to ensure it continues to meet business needs and statutory requirements.
- Assign responsibility to individuals to ensure retention periods are adhered to.
- Ensure the methods of destruction are appropriate to prevent disclosure of personal data during and after disposal e.g. for paper documents cross shredding or incineration either in-house or by a third party, for electronic documents deletion from systems or "put beyond use" and for hardware degaussing or destruction (shredding).
- Provide facilities for collecting and holding confidential personal data prior to disposal with instructions regarding how and when these should be used.

Guidance

Deleting personal data, ICO **www.ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf**

Retaining personal data, in ICO guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/**

Disposal of records, National Archives **www.nationalarchives.gov.uk/documents/information-management/rm-code-guide8.pdf**

Dispose of information you no longer need, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/stage-4-dispose-information-longer-need**

Disposing of records, National Archives **www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal**

Notes

GDPR Checklist CCTV

Notes

GDPR Checklist – CCTV

This GDPR checklist has been created by the ICO (Information Commissioners Office) to help prepare businesses for the new data protection laws due to come in to force on 25th May 2018. We believe this to be a useful tool for our members and non-members and for all small to medium sized organisations from the private, public and third sectors.

Effective information handling makes good business sense. You will enhance your business's reputation, increase customer and employee confidence and, by making sure personal information is accurate, relevant and safe, save both time and money.

Checklist for businesses operating CCTV

GDPR covers the use of CCTV (Closed Circuit Television), which is used for a number of monitoring and surveillance purposes within small businesses and, in particular, retailers. This checklist helps you to assess the compliance of your CCTV systems including the installation, management, operation, public awareness and signage.

If you would like to complete this online checklist please visit **www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/cctv/**

On completion, a short report will be created suggesting practical actions you can take to ensure you are compliant with the GDPR. It will also provide links to additional guidance that will help ensure your business meets the new data protection laws.

Do you process personal data as a data controller or a data processor?

Before you undertake the GDPR checklist you should first determine whether your role in the process is as a data controller or as a data processor.

The definition of the two terms are:

Data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is, or will be processed.

Data processor is responsible for processing personal data on behalf of a controller. If you are processor, the GDPR places specific legal obligations on you. For example, you will be required to maintain records of personal data and processing activities and you will have legal liability if you are responsible for a breach

In some instances, an organisation will process personal information as both a data controller and a data processor. When this is the case, the ICO would advise that both assessments for a controller and processor are completed. Access to both checklists can be found here:

www.ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

Step 1: Installing a system

1.1 Privacy impact Assessment

Your business decided to install CCTV cameras as the best solution to a clearly defined problem. Your business regularly reviews whether CCTV is still the best solution to the problem. Your business has identified and documented the potential impact on individuals' privacy and taken this into account when installing and operating the system. For example, you have positioned cameras to avoid capturing images of people not visiting your premises.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

If your cameras are likely to overlook any areas which people would regard as private (e.g. a neighbour's garden), you should consider where to install them and avoid siting cameras in these locations, or restrict their fields of view or movement to minimise intrusion.

For internal workplace cameras, consider the greater expectation of privacy in certain areas such as locker rooms or social areas.

Consider the differing impacts of camera technologies. For example, a fixed camera might be more appropriate than a Pan-Tilt-Zoom and a system that records sound will be significantly more intrusive and harder to justify than one without that capability.

If your business is sited in a mixed or multiple-use location, consider the privacy concerns of the users of any common spaces.

Refer to the CCTV code of practice pages 8-14 and 23-25 **www.ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf**

Suggested actions

- Review whether CCTV cameras are required to address a particular issue faced by your business.
- Consider whether alternative solutions might be more suitable.
- If you have decided to install CCTV then undertake a Privacy Impact Assessment to consider and address any privacy concerns.

Guidance

CCTV code of practice, pages 8-14 and 23-25, ICO **www.ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf**

Privacy impact assessment code of practice, ICO **www.ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf**

Privacy by design, ICO Guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/**

Employment, ICO Guide to data protection **www.ico.org.uk/for-organisations/guide-to-data-protection/employment/**

Employment practices code, ICO **www.ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf**

Employment practices code supplementary guidance, ICO **www.ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf**

Refer to the CCTV code of practice pages 8-14 and 23-25 **www.ico.org.uk/media/for-organisations/documents/1066/employment_practice_code_supplementary_guidance.pdf**

1.2 Registration

Your business has registered its CCTV processing with the Information Commissioner's Office (ICO).

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

If you process CCTV images of individuals, your business needs to record this on the public register of data controllers.

This is called 'registration' and you should renew and update it annually. Your registration should include the reasons you use CCTV, who you might share the images with and any other relevant details.

If you have an existing registration, you will need to update this to include CCTV. You should record the next renewal date.

Suggested actions

If you are processing personal data within your business, you must register with the Information Commissioner's Office (ICO) unless you are exempt. Failure to do so is a criminal offence.

You should ensure that:

- Your registration records the types of personal data (including CCTV images) your business holds and why.
- You renew each year so that the details can be recorded on the public register of data controllers.

Guidance

Register (notify) under the Data Protection Act, ICO **www.ico.org.uk/for-organisations/register/**

Registration FAQs, ICO **www.ico.org.uk/for-organisations/register/faqs/**

Step 2 of 4: Management

2.1 Governance

Your business has a policy and/or procedure about the use of CCTV. Your business has nominated an individual who is responsible for the operation of the CCTV system.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

A policy will help you to use CCTV consistently. The policy should cover the purposes you are using CCTV for and how you will handle this information, including guidance on disclosures and recording them.

It is good practice to assign day-to-day responsibility for CCTV to an appropriate individual. They should ensure that your business sets standards, has procedures and that the system complies with legal obligations including individuals' rights of access.

Suggested actions

You should:

- Ensure that there is a policy in place to allow you to use CCTV consistently.
- The policy should identify clearly defined and specific purposes for the use of CCTV information and include or refer to clearly documented procedures on how this information should be handled.
- It could include guidance on disclosures and how to keep a record of these.

Guidance

Refer to the CCTV code of practice, pages 10-12, ICO **www.ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf**

2.2 Requests for personal data

Your business has established a process to recognise and respond to individuals making requests for copies of their own images and to seek prompt advice from the Information Commissioner where there is uncertainty. Your business does not provide images to third parties other than law enforcement bodies.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Be aware of people's right to request a copy of their image (including staff) and be prepared to deal with these. These rights exist for both staff and customers.

Have a clear policy already in place that will help you deal with requests much more effectively.

An individual should not have any greater difficulty in requesting their data when this is an image compared to a document or computer file.

Providing information promptly is important, particularly if you have a set retention period which conflicts with the statutory 40 calendar day response period. In such circumstances it is good practice to put a hold on the deletion of the information.

When dealing with subject access requests you should carefully consider information about third parties, just as you would be if they were mentioned in a document or computer file that was the subject of a request.

Keeping an accurate log of subject access requests you receive and how they have been handled is valuable in helping manage requests and in case your handling is challenged.

Suggested actions

You should:

Establish a clear process for staff to follow when handling requests from individuals who wish to access copies of their own images. The process should help staff to:

- Recognise a request.
- Identify and obtain the requested footage.
- Provide the requested information in a secure and approved manner.
- Keep the necessary records about a request and how it was handled.
- Seek advice where necessary, whether internally or from the ICO.

Guidance

Refer to the CCTV code of practice pages 17-18 **www.ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf**

Subject access requests, ICO **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/**

2.3 Training

Your business trains its staff (to ensure that they have sufficient understanding of how) to operate the CCTV system and cameras (if applicable). Your business trains its staff to recognise requests for CCTV information/images.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Make all relevant staff aware of your CCTV policy and procedures and train them where necessary.

For example:

- All staff who are authorised to access the cameras should be familiar with the system and with the processes for reviewing footage and extracting it if required.
- All staff should be familiar with procedures for recognising and dealing with requests for personal data.
- All staff should be familiar with the likely disciplinary penalties for misuse of the cameras.
- Where a staff member's role explicitly includes monitoring of CCTV – for example a security guard, ensure that appropriate training standards are met and recorded (such as SIA qualifications).

Refer to the CCTV code of practice pages **www.ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf**

Suggested actions

You should:

- Ensure that all staff who are authorised to access the cameras are familiar with the system, and with the processes for reviewing footage and extracting it if required.
- Ensure that all staff are familiar with the likely disciplinary penalties for misuse of the CCTV systems.
- Where a staff member's role explicitly includes monitoring of CCTV, for example a security guard, ensure that appropriate training standards are met and recorded (such as SIA qualifications).

Step 3 of 4: Operation

3.1 Retention

Your business only retains recorded CCTV images for long enough to allow for any incident to come to light (e.g. for a theft to be noticed) and to investigate it.

- ○ Not yet implemented or planned
- ○ Partially implemented or planned
- ○ Successfully implemented
- ○ Not applicable

You should retain data for the minimum time necessary for its purpose and dispose of it appropriately when no longer required. The retention period should not be based merely on the storage capacity of the system, but reflect how long the data is needed for the purpose.

You may need to retain information for a longer period, if a law enforcement body is investigating a crime and asks you to preserve it, to give them opportunity to view the information as part of an active investigation.

You should delete it when it is not necessary to retain, for example, it does not achieve the purpose for which you are collecting and retaining information.

You should implement controls including:

- Document your information retention policy for CCTV information and ensure it is understood by those who operate the system.
- Implement measures to ensure the permanent deletion of information through secure methods at the end of the retention period.
- Undertake systematic checks to ensure that the retention period is being complied with in practice.

In addition it is worth noting that long retention periods can affect the quality of the footage with modern cameras recording to hard disks.

Suggested actions

You should:

- Document your information retention policy for CCTV information and ensure that it is understood by those who operate the system.
- Implement measures to ensure the permanent deletion of information through secure methods at the end of the retention period.
- Undertake systematic checks to ensure that the retention period is being complied within practice.

Guidance

Refer to the CCTV code of practice pages page 20-21 **www.ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf**

Retaining personal data (Principle 5), ICO **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/**

3.2 Data quality

Your business has selected a system which produces high quality, clear images which law enforcement bodies (usually the police) can use to investigate crime. Your business can easily extract these images from the system when required. Your business has sited its CCTV cameras to ensure that they provide clear images. Your business carries out regular checks to ensure that the system is producing high quality images.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Ensure the quality of the footage is fit for purpose and ensure that system settings do not compromise quality. For example, on a modern digital system ensure the overwrite cycle is not too long and degrades footage as the system trades resolution for recording time. Be aware of tree and plant growth or other obstructions which might interfere with cameras' views.

Suggested actions

You should:

- Review your business's CCTV system to ensure that it is fit for purpose.

You must sufficiently protect all information to ensure it does not fall into the wrong hands.

Poor security can lead to your cameras' feeds being viewed by criminals or being hijacked by them for use in computer botnets.

This should include technical, organisational and physical security. For example you should:

- Implement safeguards to protect wireless transmission systems from interception.
- Restrict the ability to make copies of information from CCTV systems to appropriate staff.
- Ensure appropriate controls are in place if the CCTV system is connected to, or made available across, a computer network.
- Maintain a secure space to the store CCTV footage.
- Train staff in security procedures.
- Apply sanctions to deter staff from misusing surveillance system information.
- Apply software updates (particularly security updates) published by the equipment's manufacturer to the system in a timely manner.

You should protect the recorded footage from a CCTV system, whether tapes or hard disk, against access by any unauthorised person, whether an unauthorised staff member or an outsider.

Store any data you have collected securely e.g. by using encryption or another appropriate method of restricting access to the information.

Guidance

Refer to the CCTV code of practice pages page 12-14 and 33-36 **www.ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf**

3.3 Data Security

Your business securely stores CCTV images and limits access to authorised individuals. Your business regularly checks that the CCTV system is working properly.

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

You must sufficiently protect all information to ensure that it does not fall into the wrong hands.

Poor security can lead to your cameras' feeds being viewed by criminals, or being hijacked by them for use in computer botnets.

Security precautions should include technical, organisational and physical security. For example:

- Protect wireless transmission systems from interception.
- Restrict the ability to view or make copies of information to appropriate staff.
- A secure space where footage is stored.
- Staff training in security procedures and sanctions against staff who misuse surveillance system information.
- Establish appropriate controls if the system is connected to, or made available across, a computer network. Internet-protocol (IP) cameras should be protected by firewall and router controls and wherever possible default passwords should be changed.
- Apply any software updates (particularly security updates) published by the equipment's manufacturer to the system in a timely manner. Modern IP camera manufacturers issue security advisories and fixes to security problems and users should keep these patched and up-to-date just as much as their other computer equipment.
- Protect the recorded footage from a CCTV, whether tapes or hard disk, and against access by any unauthorised person, whether an unauthorised staff member or an outsider.
- Store any data you have collected securely e.g. by using encryption or another

Suggested actions

You must sufficiently protect all information to ensure it does not fall into the wrong hands.

Poor security can lead to your cameras' feeds being viewed by criminals, or being hijacked by them for use in computer botnets.

This should include technical, organisational and physical security. For example you should:

- Implement safeguards to protect wireless transmission systems from interception.
- Restrict the ability to make copies of information from CCTV systems to appropriate staff.
- Ensuring appropriate controls are in place if the CCTV system is connected to, or made available across, a computer network.
- Maintain a secure space to the store CCTV footage.
- Train staff in security procedures.
- Apply sanctions to deter staff from misusing surveillance system information.
- Apply software updates (particularly security updates) published by the equipment's manufacturer to the system in a timely manner.

You should protect the recorded footage from a CCTV system, whether tapes or hard disk, against access by any unauthorised person, whether an unauthorised staff member or an outsider.

Store any data you have collected securely e.g. by using encryption or another appropriate method of restricting access to the information.

Guidance

Refer to the CCTV code of practice pages page 12-13 and 21-23 and 33-36 **www.ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf**

Step 4 of 4: Public awareness and signage

4.1 Fair processing

Your business clearly displays signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system, contact details are displayed on the sign(s). Your business outlines the use of CCTV and its purposes on its website (where applicable).

- ◯ Not yet implemented or planned
- ◯ Partially implemented or planned
- ◯ Successfully implemented
- ◯ Not applicable

Make signs the right size and location so that a person is aware that they are being observed and given as much warning as possible. Such transparency may also have a deterrent effect in itself.

Suggested actions

- Put clearly visible signs in place to ensure that anyone likely to be captured by the cameras is aware of them.
- Ensure that signs include the contact details for the system's owner.
- Consider including a web address where you can provide more detailed information about the system.

Guidance

Refer to the CCTV code of practice pages page 38 **www.ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf**

Processing personal data fairly and lawfully (Principle 1), ICO **www.ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/**

Privacy notices code of practice, ICO **www.ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/**

GDPR Templates

Notes

Data Protection Policy – GDPR

Date of publication: 4th April 2018

Date of Review: 4th April 2020

Responsibility: [Name], Data Protection Policy

Rationale

The Forum of Private Business ([Company name]) is committed to a policy of protecting the rights and privacy of individuals, including members, staff and others, in accordance with the *General Data Protection Regulation (GDPR) May 2018*.

The new regulatory environment demands higher transparency and accountability in how membership organisations use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that [Company name] will need to be aware of as data controller and processor, including provisions intended to enhance the protection of members' personal data. For example, the GDPR requires that:

We must ensure that our privacy notices are written in a clear, plain way that staff and members will understand.

[Company name] needs to process certain information about its staff, [customers / members] and others with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of staff.

2. The administration of [Services].

3. Provide [specific to your business].

5. Recording [specific to your business] for legal and contractual obligations.

6. Collecting fees.

7. Complying with legal obligations to funding bodies and government including local government.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR), [Company name] must ensure that all this information about individuals is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Compliance

This policy applies to all staff and members of [Company name]. Any breach of this policy or of the Regulation itself will be considered an offence and the disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with [Company name], and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR)

This piece of legislation comes in to force on 25th May 2018. The GDPR regulates the processing of personal data and protects the rights and privacy of all living individuals (including children), e.g. by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files, electronic records, photographs, CCTV images) and may include facts or opinions about a person.

For more detailed information on these regulations see the *Data Protection Data Sharing Code of Practice* (DPCoP) from the Information Commissioner's Office (ICO). Please follow this link to the ICO's website (**www.ico.gov.uk**)

Data protection principles

The legislation places a responsibility on every data controller and data processor to process any personal data in accordance with the eight principles. More detailed guidance on how to comply with these principles can be found in the DPCoP. Please follow this link to the ICO's website (**www.ico.gov.uk**) In order to comply with its obligations, [Company name] undertakes to adhere to the eight principles:

1. Process personal data fairly and lawfully.

[Company name] will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller/data processor, the purposes of the processing, any disclosures to third parties that are envisaged, given an indication of the period for which the data will be kept and any other information which may be relevant.

2. Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

[Company name] will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3. Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

[Company name] will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4. Keep personal data accurate and, where necessary, up to date.

[Company name] will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify [Company name] if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of [Company name] to ensure that any notification regarding the change is noted and acted on.

5. Only keep personal data for as long as is necessary.

[Company name] undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation and any other statutory requirements. This means [Company name] will undertake a regular review of the information held and implement a weeding process.

[Company name] will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6. Process personal data in accordance with the rights of the data subject under the legislation.

Individuals have various rights under the legislation including a right to:

- Be told the nature of the information [Company name] holds and any parties to whom this may be disclosed.
- Prevent processing likely to cause damage or distress.
- Prevent processing for purposes of direct marketing.
- Be informed about the mechanics of any automated decision making process that will significantly affect them.
- Not have significant decisions that will affect them taken solely by automated process.
- Sue for compensation if they suffer damage by any contravention of the Legislation.
- Take action to rectify, block, erase or destroy inaccurate data.
- Request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

[Company name] will only process personal data in accordance with individuals' rights.

7. Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

[Company name] will ensure that all personal data is accessible only to those who have a valid reason for using it.

[Company name] will have in place appropriate security measures examples which will include but are not limited to:

- Keeping all personal data in a lockable cabinet with key controlled access.

- Password protecting personal data held electronically.
    - Holding all [Customer] data on a secure [CRM system].
    - Ensuring any data sent to third parties for the purposes of [specify to company] is sent in a secure and encrypted manor.
- Archiving personal data which is then kept securely.
    - Annually deleted aged/ irrelevant data/incorrect data.
        - Placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
        - Ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, [Company name] will put in place appropriate measures for the deletion of personal data. Manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and third parties who process personal data 'offsite', e.g. when working at home and in circumstances additional care must be taken regarding the security of the data.

8. Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

[Company name] will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet, as because transfer of data can include placing data on a website that can be accessed from outside the EEA, therefore so [Company name] will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If [Company name] collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website and wherever else personal data is collected.

Consent as a basis for processing

Although it is not always necessary to gain consent from an individual before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when[Company name] is processing any sensitive data, as defined by the legislation.

[Company name] understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. [specify to company]) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

Personal Details

- *For the purposes of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 you consent to the College holding and processing personal data including sensitive personal data of which you are the subject, details of which are specified in the College's data protection policy.*
- *This will include marketing images and the College CCTV.*

[Company name] will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

[Company name] will ensure that if the individual does not give his/her consent for the processing and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Subject access requests

Individuals have a right to access any personal data relating to them which are held by [Company name]. Any individual wishing to exercise this right should apply in writing to the DPO. Any member of staff receiving a SAR should forward this to the DPO.

Under the terms of the legislation, any such requests must be complied with within 30 days.

Disclosure of Data

Only disclosures which have been notified and agreed with the approved and authorised third parties must be made and therefore staff should exercise caution when asked to disclose personal data held on another individual or third party.

[Company name] undertakes not to disclose personal data to unauthorised third parties, including unnamed employees of members.

Legitimate disclosures may occur in the following instances:

- The individual has given their consent to the disclosure.
- The disclosure is in the legitimate interests of the [customer].
- The disclosure is required for the performance of a contract.
    - The disclosure is a legal obligation.
    - The disclosure is the public interest.

In no circumstances will [Company name] sell any of its databases to a third party.

Data Retention Policy – GDPR

Date of publication: 11th April 2018

Date of Review: 11th April 2018

Responsibility: [Name], Data Protection Officer

[Company name] *is hereinafter referred to as "the company"*

Overview

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the company's guidelines on retention are consistently applied throughout the organisation.

Purpose

The purpose of this policy is to specify the company's guidelines for retaining different types of data.

Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location.

Note that the need to retain certain information can be mandated by local, industry regulations and will comply with *EU General Data Protection Regulation GDPR* and the *Data Protection Act 1988* and the *Data Protection (Amendment) Act 2003*. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

Policy

4.1 Reasons for data retention

The company does not wish to simply adopt a "save everything" approach. That is not practical or cost effective and would place an excessive burden on company and IT staff to manage the constantly growing amount of data.

Some data, however, must be retained in order to protect the company's interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:

- Litigation
- Incident investigation
    - Tax/financial purposes
- Security incident investigation

- Regulatory requirements
- Intellectual property preservation
    - Contractual obligations
    - Legitimate business interests.

4.2 Data duplication

As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server and again on a backup system. When identifying and classifying the company's data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

4.3 Data retention requirements

This section sets guidelines for retaining the different types of company data.

- Personal customer data: Personal data will be held for as long as the individual is a customer of the company plus 6 years.
- Personal employee data: General employee data will be held for the duration of employment and then for 6 year after the last day of contractual employment. Employee contracts will be held for 6 years after last day of contractual employment.
- Tax payments will be held for 7 years.
- Records of leave will be held for 3 years.
- Recruitment details: Interview notes of unsuccessful applicants will be held for 1 year after interview. This personal data will then be destroyed.
- Planning data: 7 years.
- Health and Safety: 7 years for records of major accidents and dangerous occurrences.
- Public data: Public data will be retained for 3 years.
- Operational data: Most company data will fall in this category. Operational data will be retained for 5 years.
- Critical data including Tax and VAT: Critical data must be retained for 7 years.
- Confidential data: Confidential data must be retained for 7 years.

4.4 Retention of Encrypted data

[You will need IT supports input here]

4.5 Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the company will use data efficiently thereby making data management and data retrieval more cost effective. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

When the retention timeframe expires, the company must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the company's management team.

The company specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself is particularly forbidden or destroying data in an attempt to cover up a violation of law or company policy.

4.6 Applicability of other policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement

This policy will be enforced by the Data Protection Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

GDPR Privacy notice

Date of publication: 4th April 2018

Date of Review: 4th April 2020

Responsibility: [Name], Data Protection Officer

[Company name] is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the *General Data Protection Regulation (GDPR).*

It applies to all employees, workers and contractors.

[Company name] is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving licence.
- Copy of passport
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- Information about your use of our information and communications systems.
- Photographs.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies e.g. CRB.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest (or for official purposes). Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations under the relevant employment laws. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing benefits to you as listed in the company handbook.
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.

- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- Preventing fraud.
- Monitoring your use of our information and communication systems to ensure compliance with our IT policies.
- Ensuring network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- Conducting data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in relation to your employment with us. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.
- Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme]. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. [We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.]

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

During the recruitment process

We are allowed to use your personal information about criminal convictions and offences to carry out our obligations .We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however, we will notify you in writing if this position changes.

Data sharing

We may have to share your data with third parties, including third party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third party service providers process my personal information?

"Third parties" includes third party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third party service providers: e.g. payroll, pension administration, benefits provision and administration and IT services.

How secure is my information with third-party service providers and other entities in our group?

All our third party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties e.g. in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the data protection officer.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from the data protection officer. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you e.g. if you want us to establish its accuracy or the reason for processing it.

- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the data protection officer in writing. No fee usually required.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact [position]. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data protection officer

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact:

[Position and contact details].

I, [employee/worker/contractor name], acknowledge that on [insert date], I received a copy of [Company name] Privacy Notice for employees, workers and contractors and that I have read and understood it.

Signature [insert signature]

Name [inset name]

FORUM of PRIVATE BUSINESS

For our members, not for profit

Making Business Better

For more information on how we can help your business simply contact our helpline team on **01565 626001**, visit our website **www.fpb.org** or email us **info@fpb.org**.

the_fpb
forumofprivatebusiness
Forum of Private Business
forumofprivatebusiness

The Forum app is available for download from the App Store and on Google Play.

Download on the App Store

GET IT ON Google Play

Forum of Private Business Ltd
Ruskin Chambers, Drury Lane
Knutsford, Cheshire WA16 6HA

Registered in England and Wales: 01329000

GDPR02/APR18