GET DATA PROTECTION RIGHT
2040 TRAINING

GDPR Audit Guide

Tim Turner

Version 2: December 2020

Contents

1 Introduction

1.1 What is an audit for?

The UK General Data Protection Regulation (GDPR) has six principles, setting out how the use of personal data should be justified, and how it should be obtained, stored, shared, used and disposed of. It contains a series of rights that the public can exercise over their data, and a variety of obligations that the organisation has to comply with in order to underpin the principles. It is vital for the organisation to know whether and how well all these elements are working to ensure that personal data is being used effectively and safely. Checking whether the GDPR is being complied with will help avoid the risk of breaches that can interfere with business processes, damage the organisation's reputation and possibly result in regulatory investigations, or even compensation claims.

An innovation introduced by the GDPR is the so-called seventh principle: "*the controller shall be responsible for, and be able to demonstrate compliance with paragraph 1*" (paragraph 1 contains the six principles). The data controller must be able to show their ability to comply. If the data controller has a Data Protection Officer, that person has a series of specific tasks, one of which is as follows:

"*to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits*"

It doesn't end there. The Data Protection Act 2018 (DPA) contains a series of safeguards and additional requirements that apply in certain situations (e.g. processing special categories data, criminal records data or applying exemptions). Although these might be less routine, it's still vital to assess whether the organisation is properly complying with them. There are also the Privacy and Electronic Communications (EC Directive) Regulations 2003 (more commonly known as PECR) which apply to consent for marketing purposes and so are inextricably linked to data protection for any direct marketing you carry out.

Your sector may have specific rules or standards about data protection, confidentiality and information security that you must also follow – for example, the Cabinet Office's approach to risk management or the NHS Data Security Toolkit. If you're unlucky enough to end up on their radar, especially if you are audited, the Information Commissioner is likely to expect to see evidence that you comply with all relevant sector standards. You need to develop your own policies and procedures for the handling of personal data so that data protection works well for your specific organisation, and you need to check that any process that you introduce is being followed and is working. For example, the GDPR does not say whether or not you should have a Bring Your Own Device Policy; that's up to you. If you decide to introduce BYOD, you have to make sure that data is processed securely. If you decide that BYOD is not for your organisations, you need to make sure that staff cannot use their own devices at work.

Your audit could look at specific processes that your organisation carries out like disclosures to third parties or subject access, or it might look at how a department or team complies with the DPA, sector standards and local policies overall. You may attempt to audit your entire organisation, but it makes sense to break it down by teams or processes.

You should be looking for existing rules or standards that are not being complied with or which do not work, gaps in the system that need to be plugged, and good practices that should at least be recognised, if not shared more widely. An audit is not about punishment, or naming and shaming. The aim is to find areas for improvement, or positives that need to be nurtured and encouraged.

Your organisation should do whatever it can to make DP standards part of the routine. Existing systems and processes should take account of the GDPR, and wherever possible, compliance should be embedded, made as seamless and integrated as possible. Some measures might need to be actively and consciously deployed. It is your role as auditor to see whether both approaches are taken when appropriate.

NOTE: the GDPR and DPA work in tandem – most activities involving personal data require you to look at the GDPR, some will also require the input of the DPA.

1.2 Defining the objective of an audit

The objectives of your audit should be as follows:

- To assess the organisation's level of compliance with the GDPR, the DPA where it applies, and other relevant laws
- To assess the organisation's level of compliance with its own data protection policies and procedures, and any relevant sector specific standards and requirements
- To identify potential gaps and weaknesses in the organisation's data protection system.
- To identify good practice, both to encourage it where it happens, and to share it with other parts of the business

The Information Commissioner sometimes implies that (and acts as if) an audit is a punishment; whatever the logic of this might be for them, creating this impression is a significant error of judgment for you. The reason why this guide exists is to help you (the DPO / DP lead / auditor / DP consultant) to get stuck into an audit that will help your organisation to avoid DP problems, using audit as a tool to dig up problems and challenges so that you can deal with them quietly and effectively.

1.3 Importance of good communication with those being audited

Auditing is a necessary part of compliance, especially for organisations that have a DPO, but it cannot be imposed without negotiation. You should discuss the audit scope and process with senior officers and ensure that the method and timing of your audit are going to happen when those participating are best places to respond.

You should also ensure that your audit takes into account any concerns that the relevant officers already have. They may already have a priority area in mind, and from a tactical perspective, you should take that opportunity and run with it. If you find a significant breach that needs immediate attention, feed that back to the highest level you can get access to, as soon as you can. Give senior management the opportunity to deal with the problem before it explodes in everyone's face.

People you will probably need to consult are:

- Senior Information Risk Owner (if you have one)
- Information Asset Owners whose assets will be covered by your audit (if you have them)
- Caldicott Guardian (if you have one)
- Heads of any affected departments
- Data Protection Officer / IG Lead (if this isn't you)
- IT Security Officer
- Records Manager

Of course, you may not have all of these people in place – for example, Caldicott Guardians are usually appointed only in organisations who deliver Health or Social Care services. If you don't have some of them in place and you're supposed to (or in the case of the SIRO, you don't need one, but you might benefit from one), this could be your first audit finding.

Let people know what you need to do, why it's important, and how they can help you by identifying key areas of data processing, thinking clearly about the risk areas and identifying possible breaches. You do not want people tidying up and telling you what they think you might want to hear. You want dirty laundry proudly on show, skeletons gleefully dragged out of cupboards. This is the organisation's opportunity to clean house with no consequences or recriminations.

This guide is not about surprise audits designed to catch people out. Your aim is to get a clear picture of why personal data is gathered, how the public are informed about this, how data is used practically within the organisation, how it is secured, how it is shared, and how it is disposed of. You should want the people that you are interviewing to cooperate, to tell you everything that you need to know willingly.

1.4 Your role as the auditor:

The key tasks for the auditor are:

- Checking whether the organisation is complying with data protection legislation and local policies
- Assessing whether staff are aware of their data protection obligations

- Agreeing suitable corrective actions or mitigations to remove non-compliances

You need to demonstrate a number of different qualities in order to audit successfully.

- Knowledge and understanding of data protection and the organisation's policies – at all stages of your audit, you need to be aware of how the organisation operates, how it handles data, and what employees' attitudes are towards confidentiality and data handling. The more detailed a knowledge you develop about what the standards are, the better able you will be to identify potential problems
- Open-minded – try to avoid going into the audit with any preconceptions about your organisation's compliance. You cannot help your organisation to improve if you have decided that it is riddled with problems or doing everything perfectly. Start your audit with a clean sheet.
- Independent – you may feel that you owe loyalty to the organisation, or that if you find evidence of non-compliance, you may end up exposing the organisation or its employees to criticism. You should set such feelings aside. Even if your audit exposes genuine problems, it is a tool to help the organisation to overcome them and learn the lessons. The biggest risk of all is that problems or risks go unaddressed, rather than that problems are unearthed. Whatever you find, you and your colleagues can deal with them, as long as you know what they are.

1.5 Your role in the organisation

If you work on your organisation's Data Protection compliance, be open-minded about your own contribution. Whether you are a full-time auditor, someone with Data Protection or Information Governance responsibilities, or an external consultant, you should not neglect what you are doing now or have been involved in.

Part of auditing is being aware of whether you have carried out all of the tasks that you yourself are expected to have done. The advantage you have if you identify anything in your own area that can be improved, you can immediately put it right.

1.6 Confidentiality

Being an auditor is a privileged position. You may find out about all aspects of the organisation's work that might not normally be known by other employees. Those who have asked you to carry out the audit (or those you have persuaded to let you do it), as well as all of the employees you speak to, need to know that anything you find out will be used only for the purposes of the audit. The GDPR and DPA give you no obligation to report any incident or breach to the Information Commissioner unless it meets the criteria set out in A33 of the GDPR.

If you tell anyone else outside of the audit process what you have learned, you may undermine your own audit, and threaten the success of audits in other organisations. Do not discuss the content of one interview in another interview. Keep all of your notes and audit documents secure at all times. Do not show them to anyone else. Do not lose them or allow them to be stolen or compromised.

If your organisation is covered by the Freedom of Information Act, your audit work may be disclosed, or your organisation may choose to publish your findings in any case. This should be an active, conscious decision, not an accident.

2 Planning your audit

In this section, you will look at the type of audit you want to carry out and find out how to do an 'adequacy audit', where you will look at the documents that the organisation already has in place.

2.1 Adequacy audit

You can't just throw the GDPR at people and expect them to absorb it. Your organisation needs some policies and procedures – perhaps corporate, perhaps local - to ensure that everyone complies with the DPA in a way that makes sense in their particular part of the organisation. You need to look at these documents before you start – if the organisation has no policies or has not properly specified what purposes it uses data for, it is unlikely that it complies with data protection. You should make sure that these issues are put right first.

This part of the process is called an 'adequacy audit'. The adequacy audit is designed to ensure that the organisation has an adequate and appropriate foundation of policies and procedures. With those in place, it is then reasonable to look at whether the organisation is living up to the standards required by the policies, whether staff are doing what you want them to do.

You will need an overall picture of how the organisation works, what aspects of the business are most likely to involve the use of personal data, and where the riskiest activities might be undertaken. You should obtain:

- Clear description of the organisation's business activities
- Organisation structure
- Organisation chart
- Records of processing activities

2.2 What is a policy?

In many years of working on data protection, I have come across many different documents with a variety of labels. It is important to work out what a document is for, what benefit it offers to the organisation. It should be obvious what job the document is doing for the organisation. Some DP policies I have seen are little more than an explicit corporate commitment to complying with Data

Protection law. There is nothing wrong with that. However, if you're going to write and disseminate a policy, it should have some sort of practical effect, so the question is whether that kind of corporate commitment will change anything within the organisation (it might, but it might not). On the other hand, a DP policy that explicitly sets out who is responsible for data protection decisions, what staff are expected to do etc. have a much more obvious practical benefit. There are all sorts of documents you might choose to introduce, but here are three useful things that they might do:

Policy: A policy sets out the organisation's position or approach on matters over which it has a choice e.g. allocating roles as described above, rules that staff are expected to follow, or information about how a certain matter is dealt with. You might set out an acceptable use policy for using the internet at work, or using mobile devices, or working from home. A policy should not just rehash what data protection says; it should tell people the way in which the organisation wants to handle what it says.

Procedure: A procedure sets out a specific set of steps that must be followed in circumstances, in particular how a thing should be done. A procedure might set out exactly how a subject access request will be dealt with, or it may give specific instructions about how to send sensitive information out of the organisation. Procedures work best in areas where you want to achieve consistency, so they are particularly appropriate for situations like incident reporting within the data controller, incident investigation, dealing with subject rights.

Guidance: Guidance is helpful information for situations where staff need to use their discretion, or where rules are impossible, but you want them to take Data Protection issues into account. Guidance may contain advice about what factors a staff member may need to take into account when they receive a request for disclosure from the police – they need to make the decision about what to do, but guidance will give them information that will help them to make a decision.

2.3 Where to start

The ideal starting point for a positive approach to data protection is a clear overview of what personal data is held for what purpose, and a clear data protection justification for each purpose. There are several different resources which might exist to give you this overview.

2.3.1 Records of processing activities (AKA RoPA)

Article 30 of the GDPR requires most organisations to create RoPA, a summary of how personal data is processed. RoPA contain the following details:

- the name and contact details of the organisation plus the names of any joint controllers with whom it is working
- the purposes for using data
- a description of the categories of data subjects and categories of personal data being used
- categories of recipients to whom personal data have been or will be disclosed
- any recipients in countries outside the EU and the safeguards in place to protect information disclosed outside the EU
- the envisaged time limits for erasure of the different categories of data
- where possible, a general description of technical and organisational security measures

Unless the organisation is exempt, the absence of RoPA is itself a breach of Article 30. Some organisations treated RoPA as a box to tick – the GDPR itself seems to imply that RoPA exist primarily for the Information Commissioner to inspect in cases of breaches or audits. However, although incomplete without other information, the RoPA is a good starting point for the organisation's attempts to tackle data protection and many organisations have used it as such. The ICO's own template for completing RoPA includes a good deal of additional information, including the lawful basis on which personal data is being processed.

2.3.2 Information Asset Register

Many organisations have for years maintained an information asset register (IAR). An information asset is a collection of information – personal or non-personal – that is used routinely by the organisation as part of its work, held in any database, record keeping system or paper file store. The GDPR does not explicitly require data controllers to identify all of their information assets. However, the Code of Practice issued under Section 46 of the Freedom of Information Act states in Section 6(1)e that all organisations subject to FOI must identify "information and business systems that hold records and provision of the resources needed to maintain and protect the integrity of those systems and

the information they contain", which effectively requires the creation of an information asset register.

In addition, some public sector organisations are required or strongly encouraged to the identify and properly manage information assets. A register of information assets will greatly assist your audit. It will be easier to see where data is stored, how it is used and shared, and how it is disposed of if you know where the data is stored in the first place. In the absence of a functioning information asset register, you should look at the key databases, records stores, and other record keeping systems that are routinely used. It is especially useful for you to know about assets used to store special categories and other sensitive personal data.

The register records what assets the organisation holds, and who is responsible for each asset (known as the 'Information Asset Owner'). The information asset approach is used to manage the risks associated with using the assets, but a detailed IAR can amount to a detailed picture of what data is held and used by the organisation. An astute organisation might combine the RoPA and IAR to create and maintain an overall picture of how data is used – many organisations who already had an IAR have adapted it to include the RoPA requirements as well. If anything like this exists, you need to consult it.

2.3.3 Information audit / data flow mapping

A third resource that might be available is the outcome of an information audit designed to capture what personal data is held, or in particular, data flow maps which show how and why personal data flows into and out of the organisation.

These three items – RoPA, IAR and data flow maps – are not mutually exclusive and can in fact be linked or even integrated into a single information resource that describes in detail how personal data is used within the organisation. As an auditor, if any or all of them are available, you should start with them to get an understanding of what is held and why.

If they are out of date, you may decide that before you carry out an audit, you remedy this situation first so you can compare what people are doing, with what the RoPA and IAR suggest that they should be doing. A lot depends on whether you think you are dealing with an organisation that is functioning normally and reasonably safely, or whether you think that there is unacceptably risky practice

at work, and it would be better to go out into the field to see how bad that practice is.

2.4 Purposes and lawful bases

The most fundamental element of Data Protection is the need to define the purpose for which personal data is used. For the processing of the data to be lawful, its use also needs to be justified under one of six lawful bases set out in Article 6 of the GDPR. If the data is special categories data (e.g. health, religion, sexual orientation), an exemption from Article 9 of the GDPR must apply. In some cases, particularly where the data is not being used with consent or for health or social care reasons, an additional legal authorisation found in Schedule 1 of the DPA might need to be identified. These are complex, technical decisions, but it is impossible to comply with the GDPR without taking them, and other elements (particularly the individual right to be provided with transparency information about how data is being used) cannot be done without knowing which condition / exemption applies.

If the organisation has not have documented these purposes and lawful bases explicitly, this is a significant threat to effective compliance. Throughout your review of documents and policies, you should ask yourself whether the organisation can explain what purposes it is using data for, and what lawful base they are relying on to process data. If it is not clear from the RoPA, IAR or similar corporate resource, this will become a vital component of any audit you carry out.

2.5 How do I know if internal policies and procedures are adequate?

Internal policies and procedures translate the principles into local practice, based on the specific work that your organisation does. They should demonstrate how rights are dealt with, and they should explain how the obligations are carried out. The most obvious sign that they are inadequate would be if they recommend or require that staff do something that would breach data protection – for example, using data in an insecure way, or ignoring an individual's explicit refusal to give consent. You need to compare the document with the data protection principles to be sure that they are not in conflict. The organisation may, of course, take a more cautious, secure approach than data protection requires, but the framework should give staff a good overall idea of what they should be doing with personal data.

It's equally important that staff are not overloaded with information that they do not need. Several of the items on the list below – the disaster recovery processes, or the incident investigation manual for example – would be aimed at a specific and almost certainly small group of staff. Procedures for dealing with reporting incidents would need to be available to every member of staff; even a cleaner or maintenance worker who does not normally handle data might find a file or a laptop and need to know what to do next.

Organisations are sometimes keen to use their policies and procedures to stress how important Data Protection is, and how seriously staff should take it. There is clearly a role for this kind of corporate commitment. However, as an auditor, what you are looking for is a working structure:

- RESPONSIBILITY: is it clear who is responsible for the various elements of the organisation's Data Protection framework, and who they report to?
- MONITORING: is it clear how those with specific roles within the framework are monitored to ensure that they are doing what they are supposed to be doing?
- STAFF BEHAVIOUR: when carrying out processes with a significant data protection or privacy impact / effect, would the average member of staff know what was required of them?
- SCOPE: are there processes or issues that the organisation clearly ought to have addressed, and have not done so?

Policies and procedures are not the only or necessarily the best way to ensure that people are acting as you would wish them to – you should be confident that the things that need to be communicated via written documents as opposed to management and supervision have been.

2.6 Identifying third party partners and contractors

As well as identifying the information assets, you should also find out which organisations you are regularly or routinely sharing personal with. The GDPR does not require data controllers to carry out data flow mapping, where the flows of personal data in and out of the organisation are all identified so that a risk assessment can be carried out on them. However, the sharing or transmission of information is probably the most significant area of risk, and you

will be able to focus your audit on the right areas if you know when and how data is shared, and with which organisations.

Before you begin the audit, you should examine which other organisations your organisation routinely shared data with. It is especially useful for you to know when and with whom sensitive personal data is shared.

2.7 Information that should be available to the public

The first Data Protection Principle requires data controllers to provide transparency information to data subjects, setting out how and why their personal data is being gathered and used as well as other contextual information. This is also known as providing a 'privacy notice'. Some of this may be done at a service or department level, and part of your audit will be to look at application forms and scripts to see if it is being done.

However, depending on who you are and what you do, some fair processing might be done at a corporate level – for example, in contracts or on your website. You should check any corporate privacy notices, privacy policies or similar documents to see whether they comply with the requirements of GDPR Articles 13 and 14, and also to decide whether they are clear and easy to read. There is a checklist for privacy notices in Appendix 3.

2.8 Do I go ahead?

If you find that the organisation's internal policies and procedures are inadequate or incomplete, there may be no point carrying out an audit in the field. If you find that employees simply do not have sufficient guidance and direction to comply properly with the DPA, you should consider carefully how to proceed.

You should probably make improvements to the policies, communicate these improved policies to employees and let the good practice settle in before you carry out an audit. You might decide to carry out some audits in teams where there are the greatest risks to see what effect the absence of proper policies is having but remember that your audit will be more about fact finding and fire-fighting at this point. The point of an audit is to test the organisation against the requirements of data protection law, so the outcome will be very different if you're looking at the state of compliance in a situation where nobody knows

what they're supposed to be doing.

2.9 Checklist

The minimum requirements are as follows. Some of these may be amalgamated into single documents or manuals – it's not important what format they exist in, as long as the organisation has made the right decisions and documented them.

Action	Done?
The organisation has registered with the ICO, unless it is exempt	
The organisation has formally appointed a DPO, unless it is exempt	
Documented process / rules in place	Held?
Records of processing activities have been created, unless the organisation is exempt	
A clear policy (or set of policies) that sets out how long data should be retained for before being disposed of, as well as clear processes for how to dispose of data safely	
Information security rules setting out rules on virus & malware prevention, software updates, firewalls, encryption and other security measures	
Disaster recovery and business continuity documents, setting out how the organisation will recover from and keep operating if its service is attacked or seriously disrupted, either deliberately or accidentally	
An acceptable use policy, setting out how staff may use electronic and other resources like email, and the internet, including whether and how they will be monitored	
Procedure for reporting information security incidents (AKA personal data breaches)	
Procedure for investigating information security incidents	
Procedure for dealing with requests for disclosure of data from other organisations – depending on the nature of the organisation, this may include specific rules on the disclosure of CCTV images	
Practical security measures for staff, including handling passwords, physical security measures in offices	
Security measures when disclosing special categories and other sensitive data (e.g. data about vulnerable people or financial data) out of the office	

If the organisation uses CCTV, a manual for the operation of the system	
Procedure for dealing with subject access requests and other data subject rights	
Guidance (at least) on when a Data Protection Impact Assessment should be triggered, and how one should be carried out	

3 Planning and conducting the audit

In this section, you will plan your audit, decide who to speak to, and what to ask them. You will look at risks and think about the questions you want to ask interviewees, as well as considering how you will handle the interviews themselves. You must be sure that you ask questions relevant to the work of the organisation, and not just questions about the application of the GDPR.

3.1 Negotiation

If you are not familiar with the team or area you are auditing, contact relevant senior officers in advance so that you know enough about what services or functions it carries out, what data it holds and how that data is used. You need to ask the right questions and concentrate on the areas with greatest risk. Therefore, you need to know how and why information is obtained, how it used and shared, where it is stored, and how it is disposed of.

Agree the scope of the audit and the methodology that you will use with the relevant senior officers. Who should approve your audit depends on your organisation's governance arrangements, but you need to know that your audit will be supported, and staff will be available for you. Audit is a crucial part of implementing and complying with the GDPR, but one of the auditor's key jobs is to ensure that the organisation co-operates and gets the benefit. The scope and timing of the audit should be negotiated and agreed with those responsible for the areas being audited. These are the people who will need to agree any improvements your audit may identify, so you need them to buy into and support the audit. Do not conduct your audit at the team or organisation's busiest times; even if it suits you, it's a terrible place to start.

You need a clear, explicit commitment to deal with what comes out of the audit from the organisation's management. They might not necessarily want to commit to accepting and implementing every recommendation without question (they don't know what kind of cheque that would be mean signing), but they have to commit to considering your recommendations in good faith and responding intelligently to what you find.

Ideally, you will audit every team that routinely processes personal data (unless it is obvious that teams handle data in exactly the same way as each other). However, this means covering the whole organisation and will depend on how

much time you have. The larger the organisation, the more impractical it might be to achieve. In any case, we recommend that you treat audit as a continuous process that goes on throughout the year, rather than a single, concentrated activity that you will carry out periodically. By making audit a routine part of your role, you can have a continual focus on the way in which data is being used.

It may also be that a continual routine audit process will be suitable in the future, but because of risks that you or your colleagues are already aware of, there may be teams or processes that you want to look at immediately.

If an incident or other issue suggests that there is a significant risk or problem that needs to be immediately addressed. The questions you will ask are very likely to be the same regardless of the scope of the audit, because your objective is always the same: to find out whether the organisation or the part you are looking at complies with the DPA and associated standards and policies.

3.2 Functional audit (AKA horizontal audit)

A functional audit examines a process that goes across the organisation, which involves different teams and individuals. It looks at each stage of the process and examines how data protection measures are implemented. A functional audit is appropriate where there is a concern that the process carries strong risks or where there has already been an incident. The process might be a business process e.g. following the process for a service from application to delivery, or DP related service like dealing with a subject access request. The advantage of a horizontal audit is that you should be able to observe a variety of different teams and situations to get a sense of how personal data is used.

3.3 Team audit (AKA vertical audit)

A team audit looks at a team within the Organisation and examines everything that it does, from gathering information to using and sharing it, storing it and disposing of it. Every aspect of the way in which the team works is examined. This approach is recommended if the team in question handles large amounts of sensitive data or has had problems or incidents already.

3.4 Arranging the audit

The main audit will include three elements

- Interviewing key staff to understand how data protection is being implemented
- Looking around the organisation premises to ensure that the environment complies with the DPA's requirements
- Carrying out focus groups with random groups of staff (alternatively, you may decide to use a survey instead of bringing staff together)

3.5 Interviews

Section 4 of this guide includes suggested questions that you will need to answer. However, you need to select the right people to speak to. Senior managers will be able to tell you what the organisation does and why; IT, security, policy, legal and compliance will be able to tell you what protective measures are in place, and anyone from the front-line services will be able to tell you what actually happens. You need to work out what mix of people will be best placed to explain how data is used.

Beyond these three areas, you should look at the Organisation's specified purposes and the organisation's functions and structure. You should select whom to interview of the basis of the following criteria:

- Which parts of the organisation are involved in obtaining and using significant amounts of personal data?
- Which individuals can set how data is obtained and used?
- Where are the areas of significant potential risk (e.g. where data is often disclosed to third parties)?

As auditor, it is your decision as to who should be interviewed. You need to decide who in the organisation is most likely to know how personal data is collected, used, shared and disposed of. An audit is not scientific. The number of people you speak to will depend on the nature of the organisation and type of work that they do.

You should not necessarily speak to the people that the team or department want you to see. Look at the organisation and how it works; decide who you need to see. You will need the support of senior managers to ensure that barriers are not placed in your way.

You may decide that speaking to managers in key areas of the business will be sufficient to understand how the Organisation operates. You must speak to those who determine the purposes for which data is processed and ensure that each relevant part of data protection and your local policies are applied once that decision has been made.

If you decide to base your audit on a representative sample of employees in each department, consider the size of the area you are looking at. You will still need to ensure that the sample includes those whose roles allow them to see how data is used, shared and stored within the area you are looking at.

Remember, the aim of these interviews is not to test the individual interviewee's understanding, but to see how data is being processed. The aim of the focus group is to see how well the average employee understands how data protection applies.

3.6 Site inspection

When you arrange the interviews, you should take the opportunity to walk around the offices, particularly if you are not familiar with them. If you are not a regular visitor to the office in question, it might be useful to walk around unannounced. This will allow you to see how the office functions in normal circumstances, and it will also be interesting to see whether anyone asks you who you are and why you are there.

It is essential in an office environment for employees to speak to and identify strangers to ensure that data or other vital assets are not stolen or accessed inappropriately. Some parts of the organisation may legitimately limit your access to certain parts of the office if they require particularly high levels of security. You should discuss these concerns, but ultimately, it should be for the department head and the SIRO to determine whether you have access should such concerns be raised.

When looking at the office, look out for the following avoidable risks:

- Computers left logged in when the user is absent
- Sensitive documents left on desks or tables when the user is absent
- Documents left uncollected on printers and photocopiers.

- Filing cabinets containing sensitive documents being left unlocked when there are no employees in attendance
- Security doors wedged open or left unlocked
- Passwords or access codes left on show

This is an important part of the process. If interviewees or focus groups give the message that the handling of personal data is safe and secure, and the working environment is confidential, you should compare that with your own experience while auditing. Does the organisation work in the way that it says it does? Some interviewees may equally give an overly negative picture, and your observations of the environment may provide a more positive impression.

3.7 Focus groups / survey

The purpose of a focus group or a survey is to find out whether ordinary members of staff know enough about confidentiality and the effect of data protection on their work. They do not need to be experts on what DP says; they need to understand how it affects what they do as individuals.

Senior officers should have ensured that training and communications to ensure that employees understand their responsibilities. These activities should be focussed on the Organisation's functions and the data that they collect to deliver them. Therefore, the questions that you ask employees should be based on the training materials and communications that have been provided.

A focus group involves gathering a representative sample of employees, and using examples and questions to prompt discussion that will allow you assess whether they understand their responsibilities. A survey takes exactly the same approach – you send a survey to a representative sample of staff or put the survey on an intranet page. A focus group can be informal and allows you to lead the discussion into unexpected or interesting areas. A survey has to be more structured, as you will have to ask specific questions so that participants are able to respond properly.

3.8 Identifying risks

You are looking at what data protection asks for and what your organisation's own procedures require and trying to find out whether employees understand

how to implement them and act in accordance with them. Some of the problems may be obvious – data is retained after it is no longer required, letters or emails frequently do not reach their intended destination, there is no clear legal basis to process personal data.

The risks themselves could come in many forms, but these are the kinds of things you should be looking out for (a more detailed list of risks can be found in Appendix 2):

- A key element of data protection or the organisation's internal policies and procedures has not been addressed or implemented properly
- The organisation does not build the DP principles into the way it plans the business, carries out procurement, works with others, or changes its working practices or services – in particular, it does not carry out Data Protection Impact Assessments regularly or consistently on new projects or procurements
- There is no a process to identify information risk proactively, and manage that risk effectively, or that process is not widely used or understood
- The organisation does not properly communicate data protection requirements and (especially) its own policies to employees through training and reminders
- The organisation does not test employees' knowledge and their understanding of local policies and procedures
- The organisation does not routinely or effectively communicate with data subjects how their data is being used
- Personal data used by the organisation is out of date, poorly maintained, excessive or inadequate
- The way the organisation stores, transmits or disseminates personal data is unsafe or badly controlled, and is likely to lead to data being lost, stolen, shared without consent or some other justification
- The organisation does not provide individuals with the information they need or request, does not respond to other rights requests, or does not respond to their complaints or enquiries, either at all, or satisfactorily
- The organisation does not properly investigate security incidents
- Managers do not check whether employees are working as they are required to

3.9 Interviewing

The purpose of your audit is to find out whether the organisation is complying with data protection. Some of the questions you will can be straightforward, closed questions, because some requirements are concrete, and will either be in place or not. However, many of the issues you need to test out will not be straightforward. The questions in this section are a guide.

You should not simply read them out; you should put them into your own words. You may not need to ask all of the questions to everyone you speak to. Think about their role, and what they are likely to know. Is there something specific that they can tell you, or an area that they are likely to have an insight into?

Put the interview at ease; ensure that interviews take place in a friendly and open atmosphere. This is not an interrogation. The interviewee should understand that your role is not to catch them out or attach blame – the aim of the audit is to ensure that the organisation complies properly with data protection and makes appropriate improvements where required. If they identify an area that is not compliant, your role as an auditor is to find a way of resolving the problem when writing your report and making recommendations to the organisation to make necessary changes – not to find someone to blame for the problem.

This is not an interrogation! Don't neglect details like ensuring the interviewee is comfortable, you offer them a drink and a biscuit, and do what you can to put them at ease. The interviewee needs to be relaxed, comfortable and in a positive frame of mind. They might have a range of concerns they are ready to go with, or you may need to coax them a little.

4 The interview

4.1 Auditor Introduction

Introduce yourself, thank them for giving up their time to participate in the Audit, and explain what you are there to do. Encourage them to speak openly and honestly and reassure them that the point of the Audit is to find out whether any improvements are needed, rather than check up on individual employees.

4.2 Let the interviewee settle in

Give the interviewee a chance to speak. Ask some simple questions such as how long they have been doing their particular job, what personal data is used in their team.

Some people will find the process of being interviewed stressful even if someone that they already know and work with is carrying the interview out. It will be more stressful if the interviewee does not know you at all. Help them to feel at ease.

4.3 Q & A

Most of the available time should be taken up with the questions you want to ask and (especially) the corresponding answers. You should try to speak as little as possible – let the interviewee answer your questions and try to record all the useful points they make. Don't interrupt, and don't rush the interviewee.

4.4 Conclusion

Make sure that you ask the interviewee if there is anything that they think you need to know. They may have some very useful information to add to your audit, and you may not have asked it. This is their opportunity to say whatever else they think should be taken into account in the audit. Thank the interviewee warmly for their time and assistance.

4.5 Questions you need answers to

Remember that you have to decide what questions each interviewee needs to be asked. It may be all of them, or it may be a selection. It is also vital that you

compare these questions to the internal policies and procedures that you have developed. You will probably need additional questions to cover certain issues, and you will need to adapt the questions because the internal policy is more specific. For example, the GDPR requires data to be accurate, but the internal policy may say how this is to be achieved. Tailor your questions to what the organisation does and who you are speaking to.

4.6 Sample questions

Accountability and Responsibility for Data

- Is someone in the team or department nominated as having responsibility for data protection and records management?
- Are there up-to-date, relevant internal policies, guidelines and procedures to protect personal data? How often are they reviewed? How are they communicated to employees?
- Is there a process to report of non-compliance or incidents? What incidents have there been? What lessons have been learned from them? Have the lessons been implemented?
- How employees educated about the importance of confidentiality, data protection in general, and internal data protection policies, procedures and guidelines? How is the effectiveness of the programme measured?
- Have any complaints about personal data been received? How are they dealt with? What lessons have been learned?
- What measures are in place to ensure that data that is to be transferred to another organisation will be processed consistently with the DPA?
- Are new projects or procurements screened to consider whether a Data Protection Impact Assessment is necessary?
- Are DPIAs carried out?
- Are information sharing agreements in place where data sharing is routine?

First & second principle issues

- Has the organisation specified and documented the purposes for which data are collected?
- Where can they be found?
- Are the conditions that allow the processing personal data (e.g.

consent, legal obligation) properly identified and understood)?
- How is transparency information been provided to data subjects? How is this done? Look at examples of where this is done. EXAMPLE: look at some application forms, webpages or scripts used to give information to individuals over the telephone
- If there is no fair processing, has an appropriate exemption been identified?
- What measures are in place to ensure that new uses of data are explained to individuals?
- Does the organisation keep evidence of consent, where it is required?
- Has that consent been properly and fairly obtained?
- What safeguards to ensure that data are disclosed to a third party only for specified purposes?

Principle 3: adequacy, relevance, excessive use of data

- What safeguards are there to limit the collection of data including personal data to that which is necessary for the specified purposes? Do internal policies and procedures emphasise the need to do so?
- Where do you make use of pseudonymisation or anonymisation?
- How do you ensure that sufficient information is available to allow fair, well-informed decisions affecting the subject to be made?

Principle 4: accuracy

- What measures are in place to ensure that Data shall be as accurate, complete, and up-to-date as is necessary for the purposes for which they are to be used? How is the effectiveness of these measures tested?
- Is data collected directly from the Individual as far as it is practicable to do so?
- Does the organisation make it easy for individuals to keep their data up to date?

Principle 5: storage limitation

- Has the organisation developed a retention, disposal and destruction

policy for personal data? Has it been implemented? Is there evidence of safe disposal?

Principle 6: integrity and confidentiality

- What measures are in place protect the data against accidental or unlawful loss, as well as unauthorised access, disclosure, copying, use, or modification? Measures should take into account:
    - The sensitivity of the data that have been collected
    - The amount, distribution, and format of the data
    - The method of storage
    - The state of technological development
    - The cost and reasonableness of implementation of the safeguards
- Are the following measures in place? You need to know about examples of these measures being carried out in practice.
    - Physical measures, for example, secured filing cabinets and restricted access to offices
    - Organisational measures, for example, security clearances and limiting access on a "need-to-know" basis either by team or individual role, depending on the nature of the data
    - Technological measures, for example, the use of passwords and encryption
- How does the Organisation ensure that personal data is safely disposed of, and in particular how does it prevent unauthorised parties from gaining access to the data before it is disposed of? NOTE: There should be a process to shred paper documents securely. If documents are not shredded immediately, they should be stored securely until they are. There should also be a process to safely dispose of any computer equipment that stores data (i.e. anything with a hard drive, and any removable media like SD cards or CDs). The organisation should keep records of what it has disposed of and when. If it uses a separate organisation to dispose of paper records or electronic equipment, it should obtain clear evidence that data has been securely disposed of.
- How do you deal with:
    - Home working
    - Mobile working
    - Sharing data with external organisations
    - Encryption of mobile devices
    - The use of staff's own devices

Individual rights

- Is there a clear process for responding to rights requests from individuals?
- What training have staff had on recognising
- Does the process include verification of the individual's identity before granting access?
- Does the Organisation have a process so that an individual can challenge the accuracy and completeness of data, and does it amend data in a reasonable time when successful challenges are received?
- If a challenge is not resolved to the satisfaction of the individual, are the subject's comments included on the record to reflect the disagreement?

Transfers of personal data outside the EEA

- Does the organisation transfer to another party outside of the European Economic Area? When does this happen? Why is the transfer necessary?
- Which safeguards have you identified to deal with the transfer?

Complaints and challenges

- Does the Organisation have a simple, accessible process in place to receive and address complaints or inquiries about their policies and procedures relating to the handling of data including personal data?
- If a complaint is justified, can the Organisation demonstrate that it has taken appropriate measures to put things right, including, if necessary, amending its internal policies, guidelines and procedures?

Specific significant Data Protection issues

Staff monitoring

- If staff are being monitored in any way, have they been informed (not necessary for specific investigations)?
- Are they aware of the standards and policies that the monitoring is intended to police?
- Was a DP impact assessment carried out to ensure that the impact of the

monitoring was proportionate?

CCTV

- Does the use of CCTV comply with the requirements of the ICO's CCTV Code of Practice?
- Are signs indicating the use of CCTV visible in the appropriate places?
- Is the storage and viewing of CCTV images done in secure circumstances?
- Is there a proper process for sharing CCTV images with the police and other investigatory authorities?

Contractors

- Is a written contract in place with every contractor or supplier that has access to your personal data?
- Does it require them to act only on your instructions?
- Have you obtained explicit and appropriately detailed security guarantees from the contractors?
- Have you ensured that security that the contractor has in place is at least as robust as that which your organisation has in place?
- Does the contract require the contractor to ensure that any sub-contractors operate the same standards, or alternatively, does it forbid the use of contractors?
- Does the contract ensure that the contractor does not use data for any other purposes?
- Does the contract ensure that data is completely disposed of at the end of the contract, and not retained in any form?

Cloud / online storage and other services

- Do you have a clear, specific contract in place with cloud / online suppliers that complies with the requirements of both the ICO's guidance, the DP principles and the requirements on contractors' above?

5 Reporting

In this section, you will write your report, identifying risks and suggesting ways in which they can be dealt with.

- Have you identified the main risks from the notes you took during the interviews?
- Have you identified a way of dealing with the risk?
- Have you drafted your report?
- Have you delivered it to the appropriate senior officer?
- Do you have a plan to deal with the identified risks, based on your discussions with appropriate senior office?

5.1 Analysing results and identifying risks

In order to determine whether the organisation is properly complying with the DPA, you need to identify risks. The standard by which you are judging the organisation is the content of the DP DPA, and by any internal policies and procedures that apply the DPA's requirements to the local environment.

Based on the information you have gathered, you need to identify any area where the organisation is not complying with the above policy framework, or is generally acting in way likely to put Data Protection and confidentiality at risk.

Appendix 2 sets out specific risks in more detail that might be present, but you must not ignore the local situation. Depending on the nature of your organisation's work, there may be vital checks carried out on data sharing, specific measures to ensure the accuracy of information, or protections on mobiles devices. You must make an assessment of the total compliance requirements and decide

5.2 Assessing the likelihood and severity of risks & risk assessment matrix

One of the most important roles of the auditor is to take what they have found out during the audit, and identify the risks associated with the Organisation's approach to data protection. They must then look at those risks and make two vital assessments:

- How severe is the possible breach likely to be, in terms of its effects on

individuals and the ability of the Organisation to carry out its role?
- How likely is it that possible breach will occur?

The risk assessment process requires you to calculate how great the risk is, based on the combination of the two factors. It is difficult to tell you how to do this; you need to examine the policy, consider the risks you have identified, and then exercise your judgement.

To determine how likely the risk is to occur, consider the following elements:

5.2.1 Likelihood of Occurrence

What is the likelihood of a breach occurring based on the identified risk or problem?

5.2.2 Impact

How would a breach of data protection in this area affect the individual or individuals, or the Organisation's ability to comply and function properly? Once you have identified the breach of data protection or of your own internal policies and procedures, you should try to identify two things; how likely is it that the breach of the policy will lead to adverse consequences, and how severe are those consequences likely to be?

Impact on the Organisation	Severe				
	High				
	Medium				
	Low				
		Remote	Unlikely	Likely	Very likely
	Likelihood that a breach will occur				

The colour coding indicates the priority with which the risk should be dealt with:

- Red: Very high priority – the breach of the policy must be dealt with immediately by changing how the organisation uses personal data
- Orange: high priority – the organisation should quickly identify a solution to the problem
- Yellow: medium priority – you should balance the risk against the effect of

correcting the breach and interfering with the work or the business
- Green: low priority – you may decide not to change the organisation's approach

5.3 Identifying your main risk treatments based on the risks

Once you have identified risks and non-compliant issues, you need to identify possible solutions. In some cases, the solution will be obvious. If you find a straightforward breach of the law or local policy, you need to suggest the best way for the organisation to make improvements. This might be through additional training and reminders for employees, giving managers more specific responsibilities to ensure that – for example – data processing purposes are specified, or individuals are properly informed.

You should not go into the audit with pre-determined solutions; the solutions you should suggest should fit the work and the culture of the organisation as well as their local policies. Training and reminders for staff are absolutely vital, and additional measures to educate employees will always be helpful. Those in management or supervisory positions should ensure that they monitor compliance with policies and procedures, and one solution to compliance issues is to make this more formal and structured.

In general, your risk treatment should fall into one of the following categories

Prevent	The risk sufficiently serious to mean that the way in which the organisation uses the data should be changed. The process should stop, or the way in which data is gathered or used should be fundamentally altered to prevent the risk from existing.
Mitigate	The risk is serious, but either prevention will damage the organisation's work in an unacceptable way, or there is an obvious step that will balance the risk out. In practice, the data continues to be gathered and used, but additional measures are put in place. Mitigation may see additional security measures, or additional measures to check that data is accurate are introduced. The risk still exists, but the mitigation will make it less likely to occur or lessen its effects.
Acknowledge / Accept	The risk is not as damaging as any solution or treatment will be to the organisation's work, or no solution can be

	identified. The risk should still be acknowledged so that the organisation is aware of the threats it faces and can keep the risk under review in case an acceptable solution can be identified in the future.

Suggested solutions can be found below, but you should not feel constrained by them. Your understanding of the organisation and its work will have a significant impact on what you think is required.

5.3.1 Information asset registers and Information Asset Owners

One approach is for the organisation to identify all the information assets (see Section 2.4.4) and compile a register. This will allow the organisation to exercise more conscious control of how data is stored, accessed and shared within and outside the organisation. Once they know what Information Assets are in use, the SIRO assigns responsibility for ensuring that the way the data in the asset is used complies. This person is known as the Information Asset Owner (IAO). Their role is to understand what information is held in the asset, what is added and what is removed, how information is transferred, who has access and why.

The SIRO can ask IAOs to carry out reviews of how the Asset is used, and to put in additional security, data quality or transparency measures.

5.3.2 Data flow mapping

Another measure that IAOs or other appropriate employees might be asked to carry out is to map flows of data within and especially outside the Organisation. The aim is to find out where personal data is routinely shared with other organisations, and to identify whether appropriate controls are in place. These could include:

- Is the data shared with consent?
- If consent is not recorded, can the organisation justify sharing without consent?
- Is the method of sharing the most secure and appropriate way of sharing?
- Are checks carried out to ensure that the sharing is safe and secure?

5.3.3 Data sharing agreements

Data sharing agreements set out a common set of rules to be adopted by organisations involved in a data sharing operation. These could well form part of a contract between organisations. Where information is to be shared on a large scale, or on a regular basis, an agreement can help Agencies to comply with both the DP Policy and their own local rules.

Data sharing agreements can set out the purposes for which data is being shared and limit the purposes for which the recipient can use personal data. They can explain how and where consent for the sharing has been recorded and set out security measures for the method of sharing and the treatment of data once it has been received. Used correctly, Data Sharing agreements can improve compliance and make the sharing of data easier and more efficient, as compliance measures can be made part of the routine.

5.3.4 DP Impact Assessment / DP by design

DPIAs are a tool used in many countries to help organisations identify the most effective way to comply with their data protection obligations and protect individuals' right to confidentiality. An effective PIA allows the organisation to identify and address problems at an early stage, reducing the costs and damage to reputation that might otherwise occur. When a service or function changes, or a new information system or database is procured, the Organisation carries out an assessment of whether the development complies with the DP Policy and its own policies. Rather than bolting on solutions to DP issues later on, the Organisation ensures that way new systems or processes are designed takes the privacy issues into account. Of course, if a new process or system is inherently compliant or causes no problems, an assessment is not necessary

5.4 Audit report template

Your audit report should include the following:

- Details of who you are and when the audit was carried out
- Scope of Audit: describe in this section which parts of the organisation was examined, summarise who was interviewed and whether focus

groups or staff surveys were used

- Audit Summary: The main section of the first page is used to summarise the results of the audit. Over time, the summary may reflect changes in the organisation's compliance or approach. It is important to ensure that the summary is evaluative as well as descriptive. The summary should not unnecessarily describe issues that the organisation is already aware of this information already.
- Organisation DP Framework: Brief description and evaluation of the Data Protection framework in terms of organisation, management and documentation at the corporate level, evaluating whether the framework is adequate
- Implementation of the DP Framework: Brief description and evaluation of how the Data Protection framework operates at departmental level and how it interfaces with the corporate level i.e. how well the teams that work within the organisation work with the SIRO and DP / IG staff in implementing the law and local policies
- Overall approach: the Audit report should summarise how the Data Protection Principles have been dealt with and evaluate any special features, instances of good or innovative practice, or any problems.
- Non-compliant issues: the report should list the major non-compliant issues, with a suggested corrective action along with each one, structured according to the priority which they should be dealt with.
- Observations: your report should include any observations of improvements or changes that are not directly linked to any specific breach of Data Protection or local policies, but which you believe will help to improve the Organisation's overall compliance or approach
- Interview summary: summaries of interviews and focus groups or surveys that show the level of employee commitment to and understanding of Data Protection and confidentiality, the quantity and effectiveness of staff data protection training
- Evaluation: overall evaluation of the effectiveness of the organisation's Data Protection framework, including compliance with the DPA and overall implementation. Comment can also be made about the confidentiality culture of the organisation, and their approach to consent, security and transparency.

5.5 What next?

Once the appropriate senior manager has received your report, the process is not over. You will need to agree what steps need to be taken as a result of receiving your report. Managers will need to decide whether your recommendations for dealing with identified risk are sufficiently robust to deal with the problem. They may decide that dealing with the risk in the way you recommend will prevent the organisation from working properly. In the end, the senior managers are responsible for compliance with data protection, and they should decide what the final risk treatment should be.

Solutions to risks should be clearly explained to the teams and employees that are going to be affected by them. There may be as much work in negotiating with and assisting teams to make changes as in the audit itself.

There should be a clear action plan to implement whatever solutions and changes have been agreed. Timescales must be attached to any change that is necessary. There should be a clear explanation for why a recommendation has not been accepted. There must be a commitment to review the outcome of the audit after a fixed period of time.

After that, where is your next audit going to be, and when?

Appendix 1: Summary of GDPR principles

1 Personal data will be processed lawfully (which means according to a set of conditions which include consent, contract and legal obligations), fairly and in a transparent manner

2 Data should be collected and used for specified purposes, and not re-used in any way that is incompatible

3 The use of personal data should be minimised wherever possible - Data should be adequate, relevant and not excessive for the purpose it was obtained for.

4 Data should be accurate and where necessary, kept up to date

5 Data should not be held any longer than necessary for the purpose

6 Appropriate measures will be in place to protect data from unauthorised access, theft, accidental loss or damage

Appendix 2: Key Risks

Possible risk
Governance
• The organisation does not provide sufficient resources to support effective compliance with data protection • The DP principles are not considered when the organisation gathers data, changes or amends its work, or develops new business processes • Key responsibilities are not allocated e.g. SIRO, information governance / DP lead, records management, information security, subject access requests • Information Assets have not been identified • Information Asset owners have not been identified • The DPO does not have a clear reporting route to the highest level of senior management • The management do not have any role in monitoring DP compliance, approving or checking DP policies or rules, or scrutinising breaches
DP by design
• There is no process to identify projects likely to require a DPIA, or where a DPIA would be beneficial • DP Impact Assessments are not carried out • DP Impact Assessments are not consistently carried out • No local policies or procedures exist • DP Policies about the organisation's use of data are not available or are out of date • DP Policies about the organisation's use of data are unclear or do not accurately reflect the way the organisation uses personal data • DP policies contradict the DPA • There is no training for staff on the DPA or information handling • The training programme is ineffective or unhelpful • Requirements from the Information Commissioner or previous audits to improve or correct compliance with the DPA are not properly implemented
First principle
• Teams within the organisation do not inform senior managers / IG leads what purposes they process personal data for • The organisation does not properly inform individuals about some or all of the purposes for which they process data • In practice, the organisation is processing data for purposes that it has not informed people about

• The organisation uses data about people without consent in circumstances where consent is the only option • Consent is obtained but it is not properly or accurately recorded • Individuals are required to give consent for the use of data as a condition for a service that should be provided to them in any case • The use of data continues after consent has been withdrawn • New purposes are not properly identified and specified
Data quality
• There is no retention or disposal policy for personal data • Data is retained after its use is no longer required • There is no process to monitor whether data is disposed of safely when no longer required • Data is not obtained directly from individuals in circumstances where they would be the most appropriate source • Inaccurate data is held and used • When an individual tries to provided updated information to the organisation, it is not recorded properly
Individual rights
• There is no process for individuals to request their data • The identity of individuals is not verified before a request is dealt with • Employees do not recognise that individuals have a right to request access to their data • There are unreasonable delays or excessive charges when individuals request access • Individuals who request access to their data do not receive it • Information is unreasonably or unjustifiably withheld when they request it from the organisation • Legitimate requests for data to be corrected are not implemented by the organisation • There are no mechanisms for complaints or enquiries to be made about the organisation's approach to Data Protection • Complaints about the way personal data are ignored or not properly responded to
International transfers
• Trans-border data transfers are not identified by the organisation • The conditions for carrying out trans-border data transfers are not carried out
Security
• There is no process for reporting incidents or possible breaches of the DPA or other information security principles

- Incidents are not identified
- Incidents are not investigated
- Sensitive information is left on show in offices (on computers, on desks, on printers or photocopiers)
- There are no procedures for checking the accuracy of information before it is sent out, and no checks on whether data is being sent to the correct destination
- Staff do not check that email or postal addresses, or phone numbers are correct before they send out information
- The identity and entitlement of third parties to receive information is not checked before it is provided to them
- The organisation does not have appropriate technical measures to protect electronic data e.g. encryption, audit trails, virus and malware prevention, firewalls, back-ups (this list is not exhaustive)
- Staff are able to connect their own electronic devices to the Organisation's network and download or upload data and files
- Paper data or files is not securely stored
- Paper data that is intended for disposal is not securely stored
- Paper data that is intended for disposal is not securely disposed of
- Electronic devices that have been used to store personal data are not securely disposed of

Appendix 3: What should my privacy notice contain?

- the identity and contact details of the data controller (which should be obvious but make it clear if not)
- If the data controller is based outside the EU, the notice should specify who their representative is so that individuals can exercise their rights
- If the data controller has one, the contact details of the data protection officer
- The purposes for which personal data is being processed
- The legal basis for the processing (i.e. from Article 6 of the GDPR, and if special categories data, the exemption from Article 9)
    - If the legal basis is legitimate interests, an explanation of what those legitimate interests are
- The identity of any organisations (or classes of organisations if there are lots of them) to whom personal data is being disclosed
- If it's happening, the fact that you intend to transfer personal data to country or international organisation outside the EEA, and the safeguards for transfer on which the organisation intends to rely
- How long the personal data will be stored for, or if that is not possible, the criteria used to determine how long it will be stored for
- The data subject's rights to access, rectification, erasure, restriction, objection and access to a portable version of some data
- If consent is being relied on, the right to withdraw consent at any time.
- The right to lodge a complaint with a supervisory authority;
- Where the subject is obliged to provide data under a statutory or contractual requirement, an explanation of the possible consequences of failure to provide such data
- The existence of automated decision-making with a significant effect on the subject, including meaningful information about the logic involved

Appendix 4: GDPR Processor checklist

A data processor may be a courier who you regularly use to transfer your records, an IT specialist coming in to work on your systems, a consultant or a contractor to whom you outsource work, projects or services. If they handle, analyse, cleanse, send out, shred or collect data for your purposes, you should ask these questions BEFORE you complete a contract. No matter how good a job your contractor does, if you do not get security protections in writing, you do not have them. They are not liable for breaches – you are.

Bear in mind that your processor must offer guarantees that they can assist you with any of the GDPR's requirements - not just with the security requirements

1) Have you got a written, binding legal contract with your processor, which sets out what the job is, and how any personal data will be used?
2) Does it include guarantees that the contractor is to act only on your instructions, and must not use personal data for any other purpose without your express permission?
3) If they are subject to any legal obligation to process or share the data for other reasons, does the agreement require them to inform you before this happens?
4) Is there a clear commitment that the processor will keep your data confidential, including the measures they will take to do so?
5) Do they have appropriate security measures, which must include at least:
    - Pseudonymisation and anonymisation where necessary
    - The ability to maintain the confidentiality, integrity, availability and resilience of information systems – this should include clear references to back-ups and business continuity processes as a minimum
    - The ability to restore availability and access to personal data quickly after an incident – you should specify how quickly you want them to be able to restore
    - They should provide evidence of a programme of regular testing, assessing and evaluating of the effectiveness of their security measures
6) Does the contract require the processor to seek your permission before taking on a sub-processor (i.e. sub-contractor), and does it require them to seek permission before changing sub-processor? Alternatively, does the contract forbid them from using sub-processors?

7) Does the contract require the processor to ensure that whatever requirements you have placed on them are passed down to sub-processor (assuming that you allow them use sub-processors)?
8) Are they capable of assisting you to respond when individuals exercise their rights – this must include requests to access records, to delete data on request under the right to be forgotten, to provide a reusable version of subject data and to rectify inaccurate data? They should be able to demonstrate their ability to do this, as well as agreeing to it in the contract.
9) Does the contract clearly define what you consider to be a security breach or incident, and does it require them to inform you of any such incidents in a specified time period?
10) Does the contract require them to assist you with impact assessments, providing you with any information (including information about their systems and processes) you may require?
11) Does the contract require the processor to delete or return all personal data at the end of the contract?
12) Does the contract require the processor to provide you with any information you need to demonstrate GDPR compliance, and to allow you to audit what they do, including inspections if you require them?
13) Have you specifically set out what security arrangements they should put in place? This will depend on the arrangement, but some examples could include:
    - Have you insisted that any laptops, pen drives or other portable media are encrypted?
    - Have you required the contractor to put in place appropriate security when moving paper records around?
    - Have you insisted on secure storage when personal data is held at their premises – does paperwork need to be locked away, is information stored on systems which have anti-virus protection, back-ups and firewalls?
14) Have you set out restrictions on what the contractor can do with the data, whom they can share it with, and which of their staff is entitled to access and use the data?
15) Have you confirmed that the contractor cannot use the data for their own purposes, and cannot disclose it to a third party without your express permission?
16) Have you put in place a mechanism to monitor the contractor's compliance with these arrangements?

OTHER THINGS TO CHECK

The GDPR gives Data Processor certain obligations that exist outside the contract with the Data Controller – you should check that the processor is complying with their obligations. Even though you as controller are not responsible, you should be aware whether they are complying.

- Article 30: they should maintain limited records of their activities as a data processor. There are exceptions to this for small organisations that are carrying out small-scale, occasional process of non-sensitive personal data, but you should expect the contract to explain why they believe themselves to be exempt
- Article 32: they should have a proper security framework as defined by GDPR
- Article 37: they may need to appoint a Data Protection Officer, depending on the nature of their work (particularly large-scale monitoring or processing of special categories data). A small data processor is very unlikely to require a data protection officer.


GET DATA PROTECTION RIGHT
2040
TRAINING