**Data Protection Audit Guidance Notes**

# Introduction

The General Data Protection Regulation, commonly known simply as the GDPR represents a significant modernisation of data protection law and one that takes into account significant new developments in technology and new uses of personal data that simply did not exist at the time of the current (until May 2018 that is) legislation, the Data Protection Act 1998.

The GDPR brings with it a number of changes and improvements to data protection law including:

- Enhanced documentation and record-keeping requirements;
- Enhanced privacy notice (or "fair processing notice") requirements;
- Stricter rules on consent to data processing;
- A new mandatory requirement to notify the ICO (and data subjects in certain cases) of a data breach;
- Enhanced rights for data subjects;
- New obligations for data processors;
- New rules requiring the appointment of Data Protection Officers; and
- New, tougher penalties for failure to comply with the law.

In addition to these headline changes, the all-important definition of "personal data" – the key subject matter of all data protection law – has expanded considerably. Under the GDPR, personal data means: "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Simply put, the definition of "personal data" under the GDPR is much wider than that under the Data Protection Act and now includes widely-used data such as IP addresses. In some cases, even data that has been pseudonymised (key-coded, for example) can still qualify if the pseudonym can be tied to a particular person.

The core principles of the GDPR set out the central responsibilities for organisations. Personal data shall be:

> a) processed lawfully, fairly and in a transparent manner in relation to individuals;
> b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
> c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
> d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
> e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and

> organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
> f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Most importantly for the purposes of the data protection audit and these guidance notes is the following statement contained in Article 5(2) of the GDPR:

> "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

An essential starting point in complying with the GDPR, and being able to demonstrate that compliance, is a data protection audit, assessing the current state of play within your business, determining the degree to which your current practices align with the requirements set down in the GDPR, and identifying areas for improvement. These guidance notes are designed to work alongside the Data Protection Audit (BS.DAT.AU.01) and provide background information and guidance for each section and question.

# Part 1. General

### 1.1 and 1.2 Business Objectives & Statutory Obligations

Questions 1.1 and 1.2 are designed to provide an overview of the business's objectives and any statutory obligations that it may be subject to. In both cases, these questions should be answered with data protection compliance in mind. If the business collects and processes personal data, understanding the business's overall objectives and having knowledge of statutory obligations specific to the business will help later in assessing whether the data collected by the business, and the business's subsequent use of that data, is justifiable.

### 1.3 Existing Policies

Question 1.3 is broken into three parts. The answers to each may require further action, for example if a particular policy has not been updated recently, or is not easily accessible by staff, consider reviewing and updating the policy and issuing copies of the updated policy to all staff.

### 1.4 Fair Processing or Privacy Notices

Question 1.4 is broken into four parts. The answers may prompt further action, for example, if fair processing notices (also known as "privacy notices") are not provided or if they have not been updated recently. If no notices are provided to data subjects, they should be implemented as a matter of priority.

In order for the processing of personal data to be fair under the law, data subjects must (in very broad terms) be given information about your business and the purpose(s) for which you are collecting and processing their personal data. The GDPR requires that such notices are clear, easy to understand, and easily accessible. Clear, plain language should be used (especially if the notice is addressed to a young audience, e.g. on a website designed for children), and it is not permissible to charge for access to privacy notices.

### 1.5 Changes to the business

Question 1.5 is broken into three sub-questions. Each asks about changes that either have been made, are currently being made, or are planned to be made that relate to data protection. As the audit is being conducted, it is important to be aware of changes to the business that may affect the answers to certain questions. It is equally important to monitor the impact (positive or negative) of any changes that are made.

### 1.6 and 1.7 Approval Schemes & Standards

A number of schemes exist that provide a seal of approval for different aspects of your business, often online. The provider of the seal will generally carry out some level of vetting in order to grant your business the seal. In theory, privacy seals and trust seals provide a certain level of guarantee about a business, reassuring customers that they follow good practices when it comes to privacy and data protection. In practice, the reliability of a seal will depend largely upon the organisation providing it.

The UK Information Commissioner's Office ("ICO") planned to introduce their own privacy seal by the end of 2016, however as of November 2017 there does not appear to have been any further progress towards implementation. These Guidance Notes will be updated accordingly if and when the ICO introduces its seal.

A number of standards exist that relate to data protection, including BS 10012:2017 "Data

Protection. Specification for a personal information management system." The British Standard is new for 2017 and includes a range of new provisions that take account of the GDPR. Standards, including those from BSI and ISO - the International Organization for Standardisation - can be valuable tools for businesses as they provide information, specifications, and guidelines to follow in order to improve performance and compliance with respect to a particular subject - in this case, data protection.

### 1.8 Employment Contracts

Data protection is important where employee data is concerned. From the very start of the recruitment process, your business will be collecting and processing personal data about employees and prospective employees. At a minimum, every employee's contract of employment should inform the employee, in broad terms, how their personal data will be used, and obtain their agreement to the collection, processing, and holding of their personal data for such use.

### 1.9 and 1.10 Additional Legislation and/or Rules

Any business collecting and processing personal data will be subject to the GDPR, but in many cases, additional legislation will apply. The Human Rights Act 1998, for example, includes the right to respect for private and family life; and the Privacy and Electronic Communications (EC Directive) Regulations 2003 set out important rules governing marketing communications, cookies and similar technologies, communication security, and customer privacy. While the main questions in the Data Protection Audit are based around the existing Data Protection Act 1998 and the new GDPR, it is nonetheless important to be aware of additional privacy and data protection obligations imposed on your business by other legislation.

In addition to legislation, certain governing bodies, trade associations, and similar entities may also have specific rules, codes of conduct, guidelines, or similar that impose specific requirements on those businesses whose activities they cover. In some cases, such rules or guidelines may simply reiterate the legislation, or may provide guidelines and best practice on how to comply. In other cases, stricter standards may be enforced.

### 1.11 and 1.12 Senior Staff Awareness and Meetings

While it is important to have a Data Protection Officer (indeed depending upon the size of the business and the data processing activities it carries out, this may be a requirement under the GDPR) or at the very least a member of staff responsible for data protection compliance, it is nevertheless important to ensure that senior staff members are also aware of the business's obligations under the legislation and of data subjects' rights. As will be noted below, data protection training should be undertaken for all staff whose work involves personal data, however senior staff would be well advised to have a more detailed understanding of how the law affects the business as a whole.

In addition to overall awareness, it is important that that awareness translates into a proactive approach to data protection within the business. Consider whether regular meetings between senior staff - particularly those with responsibility for data protection matters - would improve your compliance.

### 1.13 ICO Registration

At present, under the Data Protection Act 1998 if your business processes personal data, unless it is exempt from the requirement, must register with the ICO. In brief, if the business only processes personal data for staff administration; accounts or records; or advertising,

marketing, and PR activities for its own purposes, it may not be required to register. Nevertheless, it is important to check with the ICO if there is any doubt.

The GDPR changes the registration requirement. The GDPR removes the requirement to "notify" the ICO of data processing, but there will be a new fee payable by data controllers to the ICO under the Digital Economy Act 2017 which, in effect, replaces the fee previously payable for registration under the Data Protection Act 1998. At the time of writing, Parliament is yet to approve the new system and fees, but these Guidance Notes will be updated accordingly when the information becomes available.

### 1.14 Data Protection Officer

Under the GDPR, certain organisations are legally required to appoint a data protection officer ("DPO"). If the organisation meets any of the following criteria, a DPO must be appointed:

- The organisation is a public authority (with the exception of courts acting in their judicial capacity); or
- The organisation carries out large scale systematic monitoring of individuals (e.g. online behaviour tracking); or
- The organisation carries out large scale processing of special categories of data (also known as "sensitive personal data") or data relating to criminal convictions and offences.

Even if your business does not meet the above criteria, however, you may still appoint a DPO to oversee compliance and awareness within the business. Irrespective of whether a DPO is appointed, however, the legal obligations imposed on your business by the GDPR remain the same.

The DPO will report to your business's highest level of management, they must be allowed to operate independently and cannot be penalised or dismissed for performing their role, and the business must provide adequate resources to enable the DPO to meet their obligations under the GDPR. A DPO does not need to have specific qualifications under the GDPR, however they must possess professional experience and knowledge and the ability to fulfil the tasks required of them by the GDPR:

- Informing their organisation and the staff within that organisation that carry out personal data processing of their obligations under the GDPR;
- Monitoring compliance with the GDPR and with their organisation's policies in relation to the protection of personal data - this includes assigning responsibilities within the organisation, raising awareness, staff training, and conducting audits;
- Providing advice (and subsequent monitoring) where requested with respect to privacy impact assessments ("data protection impact assessments" in the GDPR) carried out concerning new 'high-risk' processing activities;
- Serving as a point of contact for the ICO, consulting, where necessary, on high-risk processing activities and other matters, and cooperating with the ICO as required.

A DPO can be appointed from your existing staff if there is already someone within your business with the suitable knowledge and experience. Furthermore, the staff-member does not need to dedicate themselves exclusively to their role as DPO provided that their other roles do not give rise to a conflict of interests. Alternatively, you may contract out the role of DPO externally. One individual can provide their services as DPO to multiple organisations.

## Part 2. Privacy by Design

### 2.1 Privacy by Design

An important aspect of the GDPR is what is known as “privacy by design”. This seeks to ensure that whenever any new means of processing personal data is devised, privacy and data protection considerations - and in particular compliance with the GDPR - form an integral part of the planning and design process. In short - your business should always take a proactive approach to compliance.

It is important to consider the approach taken within your business to all new projects that use personal data in some way. If privacy and data protection does not form a key part of the design and planning process, consider revising your approach and in particular raising awareness of the business’s data protection obligations among those staff responsible for such projects.

### 2.2 and 2.3 Privacy Impact Assessments

Privacy Impact Assessments (or “Data Protection Impact Assessments” as they are known in the GDPR) form an important part of the privacy by design approach and should be carried out in the early stages of a new project that involves the use of new technologies and the processing of personal data where that processing is likely to result in a high risk to the rights and freedoms of individuals. The answers to the questions in this section of the audit should help to determine whether PIAs are being carried out where appropriate, or where there may be gaps in your privacy by design approach.

PIAs should contain the following information:

- A description of the processing operations and the purposes for which the personal data is to be processed including, where appropriate, the legitimate interests pursued by the data controller;
- An assessment of the necessity and proportionality of the data processing with respect to the purpose(s);
- An assessment of the risks to data subjects; and
- Details of the measures in place to address the risks.

## Part 3. Staff Awareness and Training

### 3.1 and 3.2 Knowledge and Questions

It is not necessary for everyone in your business to have a textbook knowledge of the GDPR, however where any individual's job role involves personal data in some way, it is important that they are aware of, and understand, the relevant aspects of the law. Maintaining such awareness should go hand-in-hand with the implementation of the other organisational measures covered by the audit.

In addition to maintaining an awareness of the specific areas of data protection law that apply to them, staff should also be aware of who to go to should they have questions about data protection. If the business has a DPO, they should be the first port of call for any staff with questions.

### 3.3 and 3.4 Staff Training

Regular training should be in place to ensure the awareness and understanding referred to under question 3.1. In some cases, particularly in a small business with few employees, it may be sufficient to provide general training to all staff. In larger organisations with more diverse roles, it may be more appropriate to provide training on specific aspects of data protection focusing on the particular roles of certain staff members. It may also be beneficial to provide data protection training to new staff (again, either to all new incoming staff or focused training based on job role).

Your goal should be to ensure that all staff members whose work will bring them into contact with personal data fully understand their obligations and the rights of data subjects under the law.

### 3.5 Departing Staff

A further point to emphasise is the importance of ongoing data protection and confidentiality on the part of any staff that have worked with personal data when they leave the business. Ensure that no copies of any personal data remain in the possession of a departing staff member and consider making a point of reminding them of their obligations prior to departure.

## Part 4. Lawfulness of Data Processing

In order for the collection and processing of personal data to be lawful under the GDPR, your business must have a lawful basis for doing so. The GDPR provides the following conditions under which personal data processing will be deemed lawful:

- You have the consent of the data subject with respect to one or more specific purposes;
- The processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract;
- The processing is necessary for compliance with a legal obligation;
- The processing is necessary to protect the vital interests of the data subject or another person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller (the business, in this case);
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller (the business, in this case) unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, particularly where the data subject is a child.

Different conditions apply if the personal data in question is sensitive personal data or, “special categories of personal data” as it is known in the GDPR:

- You have the explicit consent of the data subject, unless reliance on such consent is prohibited by law;
- The processing is necessary for carrying out obligations under employment law, social security or social protection law, or under a collective agreement;
- The processing is necessary to protect the vital interests of the data subject or another person where the data subject is incapable, physically or legally, of giving consent;
- The processing is carried out by a non-profit organisation with an aim that is political, philosophical, religious, or trade union-related, provided that the processing relates only to members or former members (or to those that have regular contact with the organisation in connection with such purposes) and provided that no data is disclosed to third parties without consent;
- The processing concerns sensitive personal data manifestly made public by the data subject;
- The processing is necessary for the establishment, exercise, or defence of legal claims, or where the courts are acting in their judicial capacity;
- The processing is necessary for reasons of substantial public interest, on the basis of EU or national law which is proportionate to the aim pursued and which contains appropriate safeguards;
- The processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of an employee, medical diagnosis, the provision of health or social care treatment or the management of health or social care systems and service on the basis of EU or national law, or a contract with a health professional;
- The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices;
- The processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR (which details safeguards and derogations relating to processing

for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes).

### 4.1 - 4.4 Purpose of Data Processing

With the above lists of lawful bases for the collection and processing of personal data in mind, the first question asks you to list the purposes for which your business uses personal data. These should be evaluated in light of the conditions set out above.

Because the rules applicable to sensitive personal data are more stringent than those applying to personal data, it is important to highlight (or keep separate) the purposes for which sensitive personal data is required.

### 4.5 Lawful Bases for Data Collection and Processing

Having compiled your list of purposes for which personal data is collected and processed by the business, each should be evaluated against the list of conditions set out above in order to determine whether there is a legal basis for using the data in that way. If the data collection and processing is made lawful on the basis of consent, further information should be provided in response to the questions that follow.

### 4.6 Consent

As outlined above, the standards of consent under the GDPR are strict; even more so where the data concerned is sensitive personal data. A key objective of the GDPR is to give data subjects more control over what happens to their personal data. This can mean more work for you as a data controller, but the benefits can go beyond technical compliance with the law, extending to greater trust and an enhanced reputation for your business.

Under the GDPR, in order to be valid, consent must be:

- Freely given;
- It must specifically cover the controller's name (i.e. your business), the purposes for which you require the personal data, and the type(s) of processing undertaken;
- Requests for consent must be prominent, separate from other terms and conditions, user-friendly, easy-to-understand, and concise;
- Obvious, requiring a positive action to opt-in (meaning that pre-checked boxes and opt-out boxes should be avoided); and
- Expressly confirmed in words.

Consent, under the GDPR must be unambiguous and involve some kind of clear affirmative action on the part of the data subject, moreover, consent mechanisms should comply with the following:

- Consent should be separate from, for example, terms and conditions. It should also generally not be a precondition to signing up for a service;
- If you use opt-in boxes to obtain consent, note that the GDPR expressly prohibits these from being pre-checked;
- The GDPR requires "granular consent" for distinct data processing operations (i.e. separate consent for different purposes); and
- Clear records must be kept in order to demonstrate consent.

It is also important to note that even once you have consent, data subjects are free to withdraw that consent at any time. You must inform data subjects of this right, and provide

easy means to exercise it. Moreover, there is no specific time limit for consent. How long it lasts will depend on the context in which it is provided. Consider this when completing Part 10, addressing the retention of personal data, below.

Having obtained consent, ensure that you have in place a suitable system for recording that consent, including the identity of the data subject, how they consented, when, to what, and what information they were provided prior to giving that consent (for example, your privacy notices).

Consent has long been an important aspect of data protection law, but the GDPR raises standards. It is therefore important to review your existing consent mechanisms in light of the new requirements and, where necessary, improve them.

As high as these standards are, it is also important to remember the other bases for lawful processing as described above. If another criterion can be satisfied, it will not always be necessary to obtain consent. For many businesses, for example, a certain amount of personal data processing will be necessary for the performance of a contract between your business and the data subject.

## Part 5. Fairness and Data Subjects' Rights

### 5.1 and 5.2 Identifying Data

Keeping in mind the purposes for your business's collection and processing of personal data, records should be kept which detail the types of personal data collected for those purposes. The information provided in this part of the audit will be important for a number of subsequent questions which will assess whether or not the data held is being held for lawful purposes and otherwise in compliance with the law.

### 5.3 Collecting Personal Data

Also useful in determining whether your business's use of personal data is appropriate and lawful is information concerning the different methods of collection as this will have a bearing on the appropriate means of obtaining consent (where necessary) and providing the required information to data subjects about their rights and your obligations.

### 5.4 The Rights of Data Subjects

This is one of the most important aspects of the GDPR as compliance with these rights is vital to ensure the protection of data subjects when it comes to the use of their personal data. Under Chapter 3 of the GDPR, data subjects have the following rights:

**The Right to be Informed**
The information you provide to data subjects must include a range of details. Such information will often be provided in your privacy statement or similar documentation. The information that must be provided will vary depending upon whether you have obtained the data from the data subject directly, or whether you have obtained it from a third party:

| Information | Obtained Directly | Obtained from Third Party |
|---|---|---|
| Identity and contact details of the data controller and the data controller's DPO. | Yes | Yes |
| Purpose of collection and processing and the lawful basis for it. | Yes | Yes |
| (Where applicable) the legitimate interests relied upon. | Yes | Yes |
| The categories of personal data. | No | Yes |
| Details of any third-party recipients of the personal data. | Yes | Yes |
| Details of any "third country" (non-EU or EEA) transfers and safeguards in place. | Yes | Yes |
| How long the data will be retained (or the criteria to determine how long). | Yes | Yes |
| The existence of data subjects' rights under the GDPR. | Yes | Yes |
| The data subject's right to | Yes | Yes |

| | | |
|---|---|---|
| withdraw consent (where applicable). | | |
| The data subject's right to complain to a supervisory authority (e.g. the ICO). | Yes | Yes |
| The source of the personal data, and whether it came from publicly accessible sources. | No | Yes |
| Whether the provision of the personal data is part of a legal or contractual requirement or obligation and the potential consequences of not supplying it. | Yes | No |
| The existence of any automated decision-making (including profiling) with details of how the decisions are made, their significance, and the consequences. | Yes | Yes |

This information should be provided at the time the personal data is obtained if it is being obtained directly from the data subject. If it is obtained from a third party, the information must be provided to the data subject within a reasonable time (not more than one month); when communicating with the data subject (if the data is being used to communicate with them); or, if the data is to be disclosed by you to another party, before that disclosure takes place.

**The Right of Access**

Data subjects have the right to access their personal data held by you along with supplementary information. In response to what is known as a Subject Access Request ("SAR") you must provide confirmation that personal data is being processed; access to the personal data you hold on the data subject; and other supplementary information (in broad terms, the same information you would be expected to provide in a privacy statement).

Under the Data Protection Act, it was permissible to charge a fee for complying with SARs - usually £10 - however the GDPR requires SAR responses to be free of charge unless the request is "manifestly unfounded or excessive" in which case a "reasonable fee" can be charged. Further copies of the same information can also be charged for.

You should respond to SARs no later than one month after receipt. In the case of complex and numerous requests, this can be extended by up to two months.

**The Right to Rectification**

Personal data should be accurate and complete (also see Part 7 below). If a data subject requests the rectification of any personal data you hold about them, this must be done within one month of their request. If the request is complex, this can be extended by up to two months.

If the personal data in question has been disclosed to any third parties, the data subject

should be informed of this.

**The Right to Erasure**

This is also known as the “right to be forgotten”. It is not an unqualified right, but in broad terms, data subjects have the right to request the deletion or destruction of personal data unless there is a sound reason for its continued processing.

The most obvious way of exercising this right is for a data subject to withdraw their consent to your use of their personal data or objects to you doing so (and there is no overriding legitimate interest that justifies continuing). Other circumstances are:

- When it is no longer necessary to hold the personal data with respect to the purpose for which it was originally collected and processed (also see Part 10 below);
- The personal data has been unlawfully processed;
- The personal data has to be erased to comply with a legal obligation;
- The data is processed in relation to the offer of information society services to a child (e.g. a social media account for a person under the age of 18) (Also note that under the GDPR, additional requirements apply to children’s personal data).

There are some circumstances in which you may refuse to erase personal data:

- When exercising the human right to freedom of expression and information;
- In order to comply with a legal obligation for the performance of a public interest task or the exercise of official authority;
- For public health purposes that are in the public interest;
- For archiving purposes that are in the public interest, scientific research, historical research, or statistical purposes; or
- For the exercise or defence of legal claims.

If any personal data affected by a request for erasure has been disclosed to a third party, that third party must also be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

**The Right to Restrict Processing**

If a data subject asserts this right, you may hold their personal data, but must not process it. In practice, this may require retaining sufficient information about the data subject so as to ensure that the restriction is respected, but no more.

The right to restrict processing applies in the following circumstances:

- If a data subject has informed you that personal data you hold about them is inaccurate, processing of that data should be restricted until its accuracy is verified;
- If a data subject objects to your processing of personal data and you are considering whether your business’s legitimate grounds for processing that data override the data subject’s interests (this applies only where the processing is necessary for the performance of a public interest task or based on legitimate interests);
- Where the processing is unlawful but rather than erasure, the data subject requests restriction; or
- Where you no longer require the personal data, but the data subject requires it to establish, exercise, or defend a legal claim.

If any personal data affected by such a restriction has been disclosed to a third party, that

third party must also be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

**The Right to Data Portability**

Data subjects, under the GDPR, have the right to obtain a copy of their personal data from a data controller in a commonly-used format and to have it transferred to a different data controller. This enables data subjects to easily re-use their personal data across different services. As with many other rights, however, this one is not unqualified. The right to data portability applies only:

- To personal data provided directly by the data subject;
- Where the personal data is being processed either with the data subject's consent or for the performance of a contract; and
- Where the processing of the personal data is carried out by automated means.

Your business must respond to requests for data portability within one month. This can be extended by up to two months where the request is complex or if you receive a number of requests.

**The Right to Object**

Under the GDPR, data subjects have the right to object to certain uses of their personal data and must be informed of the right clearly, explicitly, and separately from other information:

***Processing based on legitimate interests or the performance of a task in the public interest or the exercise of official authority (including profiling)***

Under this heading, data processing must stop unless you can demonstrate compelling legitimate grounds to continue which override the interests, rights, and freedoms of the data subject. Alternatively, you may continue if the processing is necessary for the establishment, exercise, or defence of legal claims.

***Direct marketing (including profiling)***

There are no exceptions under this heading. If you receive an objection to processing for this reason, you must cease straight away.

***Processing for the purposes of scientific or historical research and statistics***

In this case, the data subject must have "grounds relating to his or her particular situation". If the processing is necessary for the undertaking of a public interest task, you do not have to comply with the objection.

***Automated Decision-Making Rights (including Profiling)***

Improvements in technology have allowed a great deal of data processing, including decision-making, to be automated. The GDPR includes rights to protect data subjects against the risk of decisions being made that may harm them in some way without human intervention.

It is important to identify what, if any, automated decision-making takes place within your business and in particular, evaluate the procedures surrounding that decision-making.

Data subjects have the right, under the GDPR, *not* to be subject to a decision if:

- The decision is based on automated processing; and
- The decision has a legal (or similarly significant) effect on the data subject.

Your procedures must ensure that data subjects are able to obtain human intervention in the decision-making process, able to express their point of view, and able to obtain an explanation of the decision that has been made and to challenge it.

The right is not unqualified, however. Firstly, it only applies if the automated decision has a legal (or similarly significant) effect on the data subject. Further, if the decision is necessary for the performance of a contract between you and the data subject (or for entering into such a contract); or is authorised by law; or if the data subject's explicit consent has been obtained, the right also does not apply.

Profiling is any form of automated processing designed to evaluate personal aspects of a data subject such as may be used for analysing:

- Job performance;
- Financial situation;
- Health;
- Personal preferences;
- Reliability;
- Behaviour;
- Location; or
- Movements.

Processing for such purposes must be fair and transparent. Suitable procedures must be used to carry out the profiling, with appropriate technical and organisation measures adopted to minimise (and correct where necessary) errors. Finally, the personal data used for profiling must be secured in a manner proportionate to the risks posed to the interests and rights of the data subjects concerned (this includes preventing discrimination).

Additional restrictions apply under the GDPR where the personal data concerns a child or are based on sensitive personal data.

### 5.5 Transfer of Personal Data

There are many reasons why your business may transfer personal data to third parties. If your business determines the purposes for collecting and processing data and the method(s) of doing so, it will be classed as a data controller. Those to whom data is transferred will generally be processors, so called because they are *processing* data on your behalf. The GDPR applies to both data controllers and data processors.

Data controllers should, under the GDPR, only use data processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of data subjects. In short, you must ensure that any third parties to whom you transfer personal data are also complying with the law.

The GDPR also places restrictions on processor's ability to sub-contract their work. Data processors must obtain written consent from data controllers before passing personal data onto another party themselves.

A contract should be in place between a data controller and any processor they appoint.

Such contracts must include the following details:

- The subject matter and the duration of the processing;
- The nature of the processing and its purpose;
- The type of personal data to be processed and the categories of data subject; and
- The rights and obligations of the data controller.

As a guide, contracts between data controllers and data processors should contain the following requirements:

- The processor acts only on the written instructions of the controller (unless required by law to act without);
- The processor ensures that people processing the personal data are subject to duties of confidentiality;
- The processor takes suitable measures to ensure that the data is processed securely;
- The processor may not engage a sub-contractor without the controller's written consent, and then not without a written contract in place with the sub-contractor;
- The processor must assist the controller, where necessary, in handling SARs and otherwise allowing data subjects to exercise their GDPR rights;
- The processor must assist the controller in meeting its obligations under the GDPR with respect to security, PIAs, and the notification of data breaches;
- At the end of the contract, the processor must delete and/or return (as requested) all personal data; and
- The processor must comply with all audits and inspections that the controller may carry out, provide the controller with any and all information required to ensure that both parties are meeting their obligations under the GDPR, and inform the controller immediately if the processor is asked to do anything that infringes the GDPR or other data protection laws (whether EU or national).

When conducting the data protection audit, is important to ensure that your business keeps track of all personal data that has been transferred to third parties (and indeed which third party or parties it has been transferred to) and why. Furthermore, ensure that data subjects are made aware of any third-party processing to which their personal data may be subject.

## Part 6. Adequacy and Relevance

The third key principle of the GDPR states that personal data collected and processed must be adequate and relevant in relation to the purpose(s) for which it is used. This is also known as the “minimisation principle”.

### 6.1 Assessing Adequacy and Relevance

When addressing the adequacy and relevance of personal data collected and processed by the business, it is important to consider whether what you are collecting, holding, and processing is absolutely necessary with respect to the purpose(s) for which you have collected it and, most importantly, the purpose(s) for which data subjects have been informed you are using it.

On the other hand, it may be that you are not getting sufficient data for the stated purpose(s), in which case the data protection audit may highlight the need to change the data that you collect.

Finally, consider carefully whether you still need the data that you have. As processes and procedures within your business change, it may be that you are still collecting and holding personal data that is no longer relevant to your work. If any type(s) of personal data are identified under this heading, these should be deleted or otherwise disposed of and collection should also cease.

### 6.2 Reviewing Data and Methods of Collection

Having assessed the current state of the personal data held by your business, it is also important to assess the procedures in place for reviewing that data for adequacy and relevance on a regular basis. Consider how frequent such reviews should be, and whether they should be prompted by other activities such as new projects utilising personal data.

## Part 7. Accuracy

Accuracy forms the basis of the fourth principle of the GDPR. Personal data must be accurate and, where necessary, kept up to date. Further, every reasonable step must be taken to ensure that any personal data that is inaccurate is corrected or erased without delay. Reasonable steps should be taken by the business to ensure that data is accurate at the time of collection, whether from data subjects directly or from third parties, as well as steps to maintain the accuracy of that data.

### 7.1 Collecting Accurate Data and Maintaining Accuracy

This section of the audit identifies the measures in place to ensure the accuracy of personal data collected and held by the business. Start by identifying what steps are taken at the time of collection to ensure accuracy, then evaluate the measures in place to keep the data accurate. Consider the type(s) of data that are used and whether they are likely to change. Addresses and other contact information may change over time, as may certain personal circumstances. Consider how you will find out about these changes. In some cases, for example, it may be appropriate to contact your customers once a year asking them to check, confirm, and/or update their personal details on your system.

### 7.2 Accuracy of Data Transferred to Third Parties

It is important to maintain the accuracy of data even if it has been transferred to a third-party processor. In addition to evaluating current methods of checking the accuracy of data prior to transfer, consider also how that accuracy is maintained after the transfer.

## Part 8. Data Transfers Abroad

Transferring data to recipients located within the UK, EU or EEA is generally much simpler from a data protection perspective than transferring to a recipient located in a country outside of those areas. The primary reason for this is that any recipient located in the UK, EU or EEA will be bound by the same rules and standards.

It should also be noted in this context that "transfer" can include electronic access across borders.

If your business wishes to transfer personal data beyond these areas, however, things become more complicated. Personal data can only be transferred if the destination country, territory, or one or more specified sectors within that country (or, if the recipient is an international organisation, that organisation) has in place an adequate level of data protection, as determined by the European Commission, or if certain other conditions are fulfilled.

### 8.1 and 8.2 Destination Country and Data Protection Laws

Begin by identifying the country or countries in which the recipients of personal data are located. If any recipient is in a non-EU or non-EEA country, the first step will be to determine whether or not that country, territory, or one or more specified sectors within that country (or the international organisation) in question ensures an adequate level of protection.

It is important to note that it is for the European Commission to determine "adequate" in this context. More information, including details of the countries currently recognised by the Commission can be obtained here (link live as of November 2017).

### 8.3 Alternative Conditions

The "other conditions" referred to above are as follows:

- You have the explicit and informed consent of the data subject to the transfer; or
- The transfer is necessary for the performance of a contract between you and the data subject or for pre-contractual steps taken at the data subject's request; or
- The transfer is necessary for the performance of a contract made in the interests of the data subject between you and another party; or
- The transfer is necessary for important public interest reasons; or
- The transfer is necessary for the establishment, exercise, or defence of legal claims; or
- The transfer is necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally unable to give consent; or
- The transfer is made from a register which, under UK or EU law, is intended to provide information to the public (and which is open to consultation either by the general public or by those able to show a legitimate interest in inspecting the register).

Transfers are also permitted if appropriate safeguards are in place. These may be provided by the following:

- An agreement between public authorities or bodies; or
- Binding corporate rules; or
- Standard data protection clauses as adopted by the European Commission; or
- Standard data protection clauses as adopted by a supervisory authority and approved by the European Commission; or

- Compliance with a code of conduct approved by a supervisory authority; or
- Certification under an approved certification scheme as provided for in the GDPR; or
- Contract clauses agreed and authorised by the relevant supervisory authority (in the UK, the ICO); or
- Provisions in administrative arrangements between public authorities or other bodies authorised by the relevant supervisory authority.

If none of the above can be satisfied, the GDPR still allows one-off or infrequent transfers of personal data which concern only a small number of data subjects in the following circumstances, provided the relevant supervisory authority (the ICO) is informed and the affected data subjects are provided with additional information:

- The transfer is not being made by a public authority exercising its public powers;
- The transfer is not repetitive;
- The personal data being transferred relates to only a limited number of data subjects;
- The transfer is necessary for the compelling legitimate interests of the organisation transferring the data, as long as such interests are not overridden by the interests of the data subject(s); and
- Having assessed all circumstances surrounding the transfer, suitable safeguards are in place by the transferring organisation to protect the personal data being transferred.

### 8.4 Checking Compliance

Regardless of which of the above grounds for third country transfers is being relied upon, it is advisable to take steps to ensure that the applicable conditions are being complied with on a regular basis. Consider whether it may be necessary to conduct data protection audits of data processors located in third countries and ensure that you have a point of contact within any recipient organisation that can assist you in ensuring compliance.

## Part 9. Record Keeping

Keeping track of the personal data collected, held, and processed by your business is vital in order to ensure full compliance with the many requirements laid down by the GDPR. Moreover, if your business has more than 250 employees, the GDPR imposes specific record-keeping requirements.

### 9.1 and 9.2 Record Keeping Requirements

Since the nature of records required will be determined in part by the size of your business, start this section by determining the total number of employees. If the business has more than 250 employees, the GDPR requires you to keep records that include the following details:

- The name and details of your business;
- The name and details of other data controllers, if applicable;
- The name and details of your representative and data protection officer, if applicable;
- The purpose(s) for which you collect and process personal data;
- The type(s) of personal data collected and processed;
- The type(s) of data subject whose data is collected and processed;
- The recipient(s) of personal data, if applicable;
- Details of any transfers of personal data made to recipients in third countries (see Part 8) including any and all documentation and safeguards in place;

- Personal data retention schedules; and
- Where possible, details of the technical and organisational security measures in place to protect personal data (see Part 11).

If the business has less than 250 employees, you are required only to keep records of personal data processing that may be considered “high risk”, for example:

- Personal data processing that could result in a risk to the rights and freedoms of data subjects; or
- Processing sensitive personal data or data concerning criminal offences and convictions.

## Part 10. Data Retention and Deletion

Personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is collected and processed.

The GDPR allows for personal data to be stored for longer periods where the data will be processed solely for archiving purposes in the public interest, or for scientific or historical research purposes, or statistical purposes subject to the requirement that technical and organisational safeguards are in place to ensure the respect for the principle of data minimisation. Examples of such measures provided in the GDPR include pseudonymisation (provided that the purposes for which the data is retained can be fulfilled). Where the purposes can be fulfilled by further processing which does not enable (or no longer enables) the data subject to be identified, the purposes should be fulfilled in that way.

In short, your business should not retain personal data that enables data subjects to be identified for any longer than necessary in light of the reasons for which you originally collected it.

### 10.1 Data Retention

In this section, refer back to the list of personal data type(s) collected and processed by your business, and the purpose(s) for which they are collected and processed. In each case, it should be established how the retention period is determined, with such methods reviewed if necessary. It is also important that retention periods are recorded which will help to ensure that no personal data is kept for any longer than necessary.

### 10.2 Reviewing Data Retention

While all retention periods should be established before any personal data is collected or processed, it is good practice to review the retention periods from time to time, even if the purposes for, and methods of, processing do not change.

### 10.3 Deletion of Personal Data

Personal data must be securely deleted or disposed of when it is no longer necessary, or when a data subject exercises their “right to be forgotten”.

If the data is stored electronically, consider what methods of secure deletion are available. Some secure deletion methods, for example, overwrite the data after deleting it, thereby reducing the likelihood that it can be recovered. The simplest form of this merely overwrites the data with zeros in a single pass. More secure methods, overwrite the data multiple times with randomised data. The greater the number of overwrites, the more secure the deletion will be (and the longer the deletion will take). Note, however, that such methods are generally more suited to traditional spinning hard disk drives. More modern solid-state storage stores data in a very different way. Secure erasure of data stored on solid state media typically involves encryption.

If the data is stored in hard copy form, forms of secure disposal typically include shredding or burning. Note, however, that not all shredders are created equal and a basic home-office machine is not likely to render your paper records unrecoverable. International Standard DIN 66399 specifies seven levels of security for shredders. Level 3 is currently recommended as a minimum level for disposing of personal data.

### 10.4 Longer Retention of Data

As noted above, certain circumstances allow for data to be retained for longer. The requirements can be complex, but of central importance, particularly in the business context, is the removal of details that enable data subjects to be personally identified. It may be the case that a business needs to retain, for example, sales figures, but those figures do not need to be associated with individual customer identification in many cases.

## Part 11. Data Security

The GDPR requires that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The level of security required will generally be proportionate to the risks posed to the rights and freedoms of data subjects. Moreover, cost considerations, the nature, scope, context, and purposes of data processing, and the current state of the art will also be factored into determining what is appropriate. Examples provided in the GDPR include:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability, and reliance of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

### 11.1 to 11.6 Physical Data

A great deal of emphasis is placed on electronic security, but a lot of personal data is still stored and processed on paper - even if only transiently. The security measures that apply to physical data storage are likely to be quite different to those that apply to electronic storage.

Begin this section by identifying the type(s) of personal data that your business stored in a physical form. This will enable you to better determine whether the answers to the following questions cover all applicable data.

A range of different organisational measures may be in place to control access to personal data stored in physical form. An important example of such measures is the granting of different access levels to staff, ensuring that only those who have a legitimate need to access the data are authorised and able to. Organisational measures should be supported by physical measures such as locked filing cabinets.

Keeping access logs can also assist in physical data security. Not only do logs help to ensure that only authorised staff members are accessing the data, but they can also be helpful in keeping track of copies of data, something that can be invaluable in tracking down missing items. In addition, consider your backup procedures. Backing up electronic data is comparatively straightforward and automated; however, backing up physical data may require more direct action such as keeping duplicate copies in an alternative location, or storing copies electronically.

### 11.7 to 11.12 Electronic Data

As with personal data stored in a physical form, this section of the audit begins again by listing data types - in this case, data stored electronically.

Also, as with physical data, organisational measures are important when it comes to the security of electronic data. Once again, different levels of access for staff will be useful, ensuring that only those who need access to certain personal data to perform their job role have access to it. This is generally easier to implement with electronic data than it is with physical data as usernames and passwords can be configured to grant access to selective

areas of a computer system on a per-user basis.

Usernames and passwords should always form a part of a strong approach to IT security, and should work alongside other important technologies such as firewalls, encryption, virus and malware protection, and regular software and security updates.

Electronic security can also be further enforced in some cases with physical security measures. Server rooms, for example, should be locked at all times with access limited to those staff members with legitimate reasons for access.

Care must always be taken when monitoring your staff's use of computers and other electronic resources, however it can also be a valuable tool, when used correctly, to enhance the security of personal data.

In addition to controlling access to personal data stored electronically, consider the measures that will be useful in protecting the data itself. Again, measures such as virus and malware protection, encryption, firewalls, and regular software and security updates are essential. Such measures should also be active as well as passive. If a user wishes to use, for example, a USB drive, it is good practice to ensure that the drive is scanned for viruses before it can be used. Strict limitations should also be placed on staff members' use of their own personal devices.

**11.14 to 11.20 System Security**

All computers and other electronic devices on which personal data can be accessed should be protected with username and password access where possible. Also, where possible, all users should have a unique username and password. Note that this may not be possible in the case of, for example, Apple iPads since the iOS operating system currently does not support multiple users. In such cases, the device should still be protected with a passcode or with biometric ID such as a fingerprint. Sharing of such devices should thus be limited to those staff with the same access levels.

Consider the rules and policies that apply to usernames and passwords. The golden rule should always apply - no sharing of login credentials for any reason. Even IT staff should not be privy to anyone's password. Consequently, ensure that a method of changing a forgotten password is in place that keeps the information private. Further important considerations include the security of passwords. Not only can some passwords be easily guessed by a human being, but the simpler the password, the more easily it can be cracked by a computer. According to howsecureismypassword.net, the password "password1" would be cracked instantly by a computer. Conversely, it would take a computer one trillion year to crack "2042GreenTree12!". Whether by means of a policy or by technical means, ensure that users are required to choose secure passwords. Passwords should also be changed regularly and many IT administrative systems allow for time limits to be set.

Different user accounts should also, in many cases, enable the implementation and enforcement of different access levels, where appropriate. Such access levels may need to be reviewed, for example, when a staff member's role changes, or when they are assigned to a new project which requires access to more, different, or even less personal data.

Additional security measures may be necessary if staff are able to access personal data from outside your business's premises. Limiting access to a company intranet site may be helpful, as are facilities such as Virtual Private Networks (VPNs) which provide a secure "tunnel" through which users can access the required data.

A further key point to consider under the heading of system security is the revocation of

access to personal data when a member of staff leaves the business or is likely to be absent for a prolonged period of time. The staff member may need to retain access to certain facilities for a period after departure, but it is highly unlikely that a compelling reason could be found to justify continued access to personal data.

**11.21 to 11.25 Devices Provided by the Business**

This section examines security measures specific to computers, laptops, and other devices such as tablets and smartphones that are provided by the business to staff. Mobile devices in particular pose a significant hazard when it comes to the security of personal data as they can be far more easily lost, stolen, or even simply left unattended and accessible to unauthorised users when compared to desktop workstations that never leave the workplace.

If personal data is accessible on such devices, it will be important to consider first of all what type(s) of data is accessible and whether that access is necessary. The same applies to personal data that is stored on laptops and mobile devices, although a stronger case can arguably made for access than it can be for storage. The mere fact that data can be accessed does not necessarily make that data available to an unauthorised user of the device, whereas data stored is potentially available to anyone with access to the device, including someone who finds it when lost or steals it.

To minimise such risks, evaluate security measures such as encryption. If a device is encrypted, even if personal data is stored on that device, it will be very difficult - in some cases practically impossible - to access that data without the requisite access credentials.

**11.26 to 11.32 BYOD**

Bring Your Own Device, or “BYOD” is exactly as it sounds. Staff members are able to use their own personal computers and other devices for work. While this provides convenience to staff and cost savings to your business, it creates potentially serious risks where data protection is concerned.

A sound first step in ensuring security in a BYOD environment is to implement a BYOD policy. A properly-drafted BYOD policy should address key aspects including employee obligations, acceptable usage, and, of course, data protection compliance.

As with business-supplied laptops and mobile devices, establish whether personal data is accessible or stored on BYOD devices and whether that access or storage is absolutely necessary. Even more so than with a business-provided laptop, it is arguable that the storage of personal data on a BYOD device may be described as undesirable at best.

In addition to the security measures that you may have in place for offsite access to personal data, consider what additional measures may be necessary for BYOD devices, such as the provision of security software and imposing requirements such as the use of encryption, secure passwords, the creation of a separate user profile or login for work purposes, and testing and approval procedures before a BYOD device can be used to access or store personal data. A further prudent measure is to keep a record of all BYOD devices in use, including details of the staff member by whom a device is used, the personal data accessible and/or stored on it, the purpose(s) for which the device and the data are used, and other valuable IT security information such as software versions and security measures implemented.

## Part 12. Data Breaches

The final part of the audit addresses data breaches. If suitable care is taken to comply with the letter and spirit of the GDPR, breaches should be minimal or non-existent. Nevertheless, it is important to be prepared to act in the event that one occurs. Depending on the nature of a breach, it may need to be reported to the ICO and, in some cases, also to the data subjects affected.

A personal data breach is defined as a breach of security which results in the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The first step is the internal identification of a data breach. In a small business with only a few employees, this may be easy to spot, but the larger the business, the more important it is that a number of people know what to look for in order that the breach may be reported to the business's DPO or other appropriate staff member as quickly as possible.

The ICO must be informed only if the breach is likely to result in a risk to the rights and freedoms of data subjects. If such a breach is not addressed, it will be likely to have a significant detrimental effect on the data subjects. Examples provided by the ICO include discrimination, reputational damage, financial loss, and loss of confidentiality. Data subjects must be informed of a breach if the breach is likely to result in a *high* risk to the rights and freedoms of the data subjects.

If a breach is sufficiently severe to warrant reporting to the ICO, it must be reported within 72 hours of the business becoming aware of it. If data subjects also need informing, this must be done without delay.

When notifying the ICO, a breach notification must include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the business's DPO (or other contact point if no DPO has been appointed);
- A description of the likely consequences of the breach; and
- Details of the measures planned and/or taken to deal with the breach including, where relevant, measures taken to mitigate any possible adverse effects.

It is important to note that failure to report a notifiable personal data breach can result in a significant fine of up to €10m or 2% of the business's global turnover.