Data Pr e Notes

Introduction

In 2018, the EU General Data Pro monly known simply as the GDPR represented a significant modernis aw and one that took into account significant new developments in t s of personal data that simply did not exist at the time of the previo Protection Act 1998. Following the UK's departure from the Europe with certain contextual alterations which change little from an SME n UK law by virtue of section 3 of the European Union (Withdrawal) own as the "UK GDPR". Together with the Data Protection Act 2018 e backbone of UK data protection legislation (in addition to other as the Privacy and Electronic Communications Regulations). Th are often collectively referred to in legal and business documents as slation".

The 2018 legislation brought wi nges and improvements to data protection law including:

- Enhanced documentation a rements;
- Enhanced privacy notice (c) requirements;
- Stricter rules on consent to
- A new mandatory requiren nd data subjects in certain cases) of a data breach;
- Enhanced rights for data su
- New obligations for data pr
- New rules requiring the app tion Officers; and
- New, tougher penalties for law.

In addition to these headline chan inition of "personal data" – the key subject matter of all data protec ed considerably. Under the Data Protection Legislation, personal d nation relating to an identified or identifiable natural person ("data s natural person is one who can be identified, directly or indirectly, in an identifier such as a name, an identification number, location dat to one or more factors specific to the physical, physiological, gene cultural, or social identity of that natural person.

Simply put, the definition of "pers ata Protection Legislation is much wider than that under old regime -used data such as IP addresses. In some cases, even data that ha (key-coded, for example) can still qualify if the pseudonym can be tie

The core principles of the UK G responsibilities for organisations. Personal data shall be:

a) processed lawfully, fairly nner in relation to individuals;
b) collected for specified, rposes and not further processed in a manner that is incomp es; further processing for archiving purposes in the public inte al research purposes or statistical purposes shall not be cons with the initial purposes;
c) adequate, relevant and sary in relation to the purposes for which they are processed;

SAMPLE

d) accurate and, where ne e; every reasonable step must be taken to ensure that perso ate, having regard to the purposes for which they are processe d without delay;
e) kept in a form which p ata subjects for no longer than is necessary for the purposes data are processed; personal data may be stored for longer p sonal data will be processed solely for archiving purposes in t fic or historical research purposes or statistical purposes su of the appropriate technical and organisational measures r R in order to safeguard the rights and freedoms of individuals
f) processed in a manner te security of the personal data, including protection agai nlawful processing and against accidental loss, destructio opriate technical or organisational measures.

Most importantly for the purposes audit and these guidance notes is the following statement contained GDPR:

> "the controller shall be res e to demonstrate, compliance with [the principles] ('accountab

An essential starting point in com ection Legislation, and being able to demonstrate that compliance, is assessing the current state of play within your business, determining ur current practices align with the requirements set down in the law for improvement. These guidance notes are designed to work alongs Audit (BS.DAT.AU.01) and provide background information and guida question.

SAMPLE

Part 1. General

1.1 and 1.2 Business Objectives

Questions 1.1 and 1.2 are design w of the business's objectives and any statutory obligations that it ma cases, these questions should be answered with data protection co business collects and processes personal data, understanding the ectives and having knowledge of statutory obligations specific to th er in assessing whether the data collected by the business, and the se of that data, is justifiable.

1.3 Existing Policies

Question 1.3 is broken into three ach may require further action, for example if a particular policy has ntly, or is not easily accessible by staff, consider reviewing and upda ng copies of the updated policy to all staff.

1.4 Fair Processing or Privacy N

Question 1.4 is broken into four pa ompt further action, for example, if fair processing notices (also know r simply "privacy information") are not provided or if they have not f no notices are provided to data subjects, they should be implemer y.

In order for the processing of pers er the law, data subjects must (in very broad terms) be given informa s and the purpose(s) for which you are collecting and processing the ata Protection Legislation requires that such notices are clear, easy t accessible. Clear, plain language should be used (especially if the r oung audience, e.g. on a website designed for children), and it is not r access to privacy notices.

1.5 Changes to the business

Question 1.5 is broken into three ks about changes that either have been made, are currently being to be made that relate to data protection. As the audit is being nt to be aware of changes to the business that may affect the answ . It is equally important to monitor the impact (positive or negative) of ade.

1.6 and 1.7 Approval Schemes &

A number of schemes exist that oval for different aspects of your business, often online. The provid ally carry out some level of vetting in order to grant your business th y seals and trust seals provide a certain level of guarantee about customers that they follow good practices when it comes to privacy practice, the reliability of a seal will depend largely upon the organisat

1.8 Employment Contracts

Data protection is important wher cerned. From the very start of the recruitment process, your busine l processing personal data about employees and prospective em n, every employee's contract of employment should inform the e , how their personal data will be

SAMPLE

used, and obtain their agreement sing, and holding of their personal data for such use.

1.9 and 1.10 Additional Legislati

Any business collecting and proc the UK will be subject to the UK GDPR, but in many cases, additio . The Human Rights Act 1998, for example, includes the right to r family life; and the Privacy and Electronic Communications (EC 2003 set out important rules governing marketing communica ilar technologies, communication security, and customer privacy. W s in the Data Protection Audit are based around the primary data pr he UK GDPR and DPA 2018), it is nonetheless important to be awa y and data protection obligations imposed on your business by othe

In addition to legislation, certain associations, and similar entities may also have specific rules, cod es, or similar that impose specific requirements on those businesses over. In some cases, such rules or guidelines may simply reiterate th ovide guidelines and best practice on how to comply. In other cases, e enforced.

1.11 and 1.12 Senior Staff Aware

While it is important to have a Data ed depending upon the size of the business and the data processing this may be a requirement under the Data Protection Legislation) o mber of staff responsible for data protection compliance, it is never ure that senior staff members are also aware of the business's oblig on and of data subjects' rights. As will be noted below, data protecti ndertaken for all staff whose work involves personal data, however s l advised to have a more detailed understanding of how the law affe ble.

In addition to overall awareness hat awareness translates into a proactive approach to data pro ness. Consider whether regular meetings between senior staff - responsibility for data protection matters - would improve your com

1.13 ICO Registration

Subject to certain exemptions, al traders processing personal data must pay a fee to the ICO. The fe Tier 1 is for "micro organisations" with a maximum turnover of £632, ar or no more than 10 members of staff. The Tier 1 fee is £40. Tier 2 m organisations" with a maximum turnover of £36 million for their fina an 250 members of staff. The Tier 2 fee is £60. Finally, Tier 3 is for " bigger than Tier 2) and carries an annual fee of £2,900.

The ICO provides a self-assessm to assist you in determining which tier, if any, you fit into.

1.14 Data Protection Officer

Under Article 37 of the UK GDPR, e legally required to appoint a data protection officer ("DPO"). If the o the following criteria, a DPO must be appointed:

SAMPLE

- The organisation is a pub xception of courts acting in their judicial capacity); or
- The organisation carries o tic monitoring of individuals (e.g. online behaviour tracking);
- The organisation carries ou of special categories of data (also known as "sensitive pers ating to criminal convictions and offences.

Even if your business does not r however, you may still appoint a DPO to oversee compliance and usiness. Irrespective of whether a DPO is appointed, however, the d on your business by the Data Protection Legislation remain the s

The DPO will report to your busine nagement, they must be allowed to operate independently and canno sed for performing their role, and the business must provide adequa the DPO to meet their obligations under the GDPR. A DPO does cific qualifications relating to data protection; however, they must p perience and knowledge and the ability to fulfil the tasks required of tion Legislation:

- Informing their organisatio that organisation that carry out personal data processing o the UK GDPR;
- Monitoring compliance w ion Legislation and with their organisation's policies in r of personal data - this includes assigning responsibilities raising awareness, staff training, and conducting audits;
- Providing advice (and sub re requested with respect to data protection impact assessr erning new 'high-risk' processing activities;
- Serving as a point of cont ng, where necessary, on high-risk processing activities and o ating with the ICO as required.

A DPO can be appointed from y e is already someone within your business with the suitable knowle rthermore, the staff-member does not need to dedicate themselves as DPO provided that their other roles do not give rise to a conflict , you may contract out the role of DPO externally. One individual ca s DPO to multiple organisations.

SAMPLE

Part 2. Data Protectio Data Protection Impact Assessments

2.1 Data Protection by Design

An important aspect of the Data P what is known as “data protection by design and default”. This seek ver any new means of processing personal data is devised, privac considerations - and in particular compliance with the Data Protect integral part of the planning and design process. In short - your s take a proactive approach to compliance.

It is important to consider the ap business to all new projects that use personal data in some way. If ion does not form a key part of the design and planning process, c pproach and in particular raising awareness of the business’s data among those staff responsible for such projects.

2.2 and 2.3 Data Protection Impa

Data Protection Impact Assessme rt of the data protection by design approach and should be carried o a new project that involves the use of new technologies and the proc where that processing is likely to result in a high risk to the rights ar s. The answers to the questions in this section of the audit should he DPIAs are being carried out where appropriate, or where there may b design approach.

DPIAs should include the following

- A description of the proces e purposes for which the personal data is to be processed inc e, the legitimate interests pursued by the data controller;
- An assessment of the ne ality of the data processing with respect to the purpose(s);
- An assessment of the risks
- Details of the measures in s.

SAMPLE

Part 3. Staff Awareness a

3.1 and 3.2 Knowledge and Que

It is not necessary for everyone ve a textbook knowledge of data protection law, however where an olves personal data in some way, it is important that they are awa the relevant aspects of the law. Maintaining such awareness sho n the implementation of the other organisational measures covered

In addition to maintaining an awar as of data protection law that apply to them, staff should also be awa d they have questions about data protection. If the business has a first port of call for any staff with questions.

3.3 and 3.4 Staff Training

Regular training should be in plac ess and understanding referred to under question 3.1. In some case l business with few employees, it may be sufficient to provide gene In larger organisations with more diverse roles, it may be more ap ining on specific aspects of data protection focusing on the particul nembers. It may also be beneficial to provide data protection trainin ither to all new incoming staff or focused training based on job role

Your goal should be to ensure tha e work will bring them into contact with personal data fully understan e rights of data subjects under the law.

3.5 Departing Staff

A further point to emphasise is the data protection and confidentiality on the part of any staff that have ata when they leave the business. Ensure that no copies of any per e possession of a departing staff member and consider making a em of their obligations prior to departure.

3.6 Home Working

If the business has introduced ho eased it) in response to the 2020 outbreak of the novel coronavirus articularly important to make staff aware of the increased risks po rotection and security. Consider refreshing training and covering ad IT security. Under normal working conditions, your IT staff would lik ecurity and maintenance (e.g. the installation of software updates oftware), but in the absence of centrally-administered devices su laptops, individual staff members may currently be taking on mor security and safety of their own equipment.

SAMPLE

Part 4. Lawfulness of Dat

In order for the collection and p data to be lawful under the data protection legislation, your busine asis for doing so. The UK GDPR provides the following conditions data processing will be deemed lawful:

- You have the consent of respect to one or more specific purposes;
- The processing is necessa f a contract with the data subject or to take steps to enter int
- The processing is necessa egal obligation;
- The processing is neces interests of the data subject or another person;
- The processing is necessa of a task carried out in the public interest or in the exercis ested in the data controller (the business, in this case);
- The processing is necessa he legitimate interests pursued by the data controller (the bus s such interests are overridden by the interests or fundamenta the data subject which require the protection of personal data ata subject is a child.

Further conditions apply if the p n is sensitive personal data or, "special categories of personal dat K GDPR:

- You have the explicit cons unless reliance on such consent is prohibited by law;
- The processing is neces ligations under employment law, social security or social pro ollective agreement;
- The processing is neces interests of the data subject or another person where the le, physically or legally, of giving consent;
- The processing is carried o sation with an aim that is political, philosophical, religious, or ovided that the processing relates only to members or forme that have regular contact with the organisation in connection provided that no data is disclosed to third parties without cons
- The processing concerns s anifestly made public by the data subject;
- The processing is neces nt, exercise, or defence of legal claims, or where the courts l capacity;
- The processing is necessa tial public interest, on the basis of EU or national law which aim pursued and which contains appropriate safeguards;
- The processing is neces of preventative or occupational medicine, for assessing th employee, medical diagnosis, the provision of health or soci management of health or social care systems and service national law, or a contract with a health professional;
- The processing is necessa terest in the area of public health, such as protecting agains reats to health or ensuring high standards of healthcare an r medical devices;
- The processing is necessa in the public interest, or scientific and historical research pu poses in accordance with Article

SAMPLE

89(1) of the UK GDPR rds and derogations relating to processing for archiving c interest, scientific or historical research purposes, or stati

4.1 - 4.4 Purpose of Data Proces

With the above lists of lawful ba d processing of personal data in mind, the first question asks you t hich your business uses personal data. These should be evaluated i et out above.

Because the rules applicable to a are more stringent than those applying to personal data, it is in keep separate) the purposes for which special category personal da

4.5 Lawful Bases for Data Collec

Having compiled your list of purpo ata is collected and processed by the business, each should be eval onditions set out above in order to determine whether there is a lega in that way. If the data collection and processing is made lawful nt, further information should be provided in response to the questi

4.6 Consent

As outlined above, the standards K GDPR are strict; even more so where the data concerned is sens y objective of the Data Protection Legislation is to give data subject t happens to their personal data. This can mean more work for y but the benefits can go beyond technical compliance with the law, st and an enhanced reputation for your business.

According to the UK GDPR, in ord ust be:

- Freely given;
- It must specifically cover t your business), the purposes for which you require the pers) of processing undertaken;
- Requests for consent mus from other terms and conditions, user-friendly, easy-to-unde
- Obvious, requiring a positi ning that pre-checked boxes and opt-out boxes should be av
- Expressly confirmed in wor

Consent must be unambiguous a clear affirmative action on the part of the data subject, moreover, con comply with the following:

- Consent should be separa rms and conditions. It should also generally not be a precond ervice;
- If you use opt-in boxes that they should never be pre-checked;
- The Data Protection Le ular consent" for distinct data processing operations (i.e. erent purposes); and
- Clear records must be kept consent.

It is also important to note that onsent, data subjects are free to

SAMPLE

withdraw that consent at any time subjects of this right, and provide easy means to exercise it. Moreo time limit for consent. How long it lasts will depend on the context in onsider this when completing Part 10, addressing the retention of per

Having obtained consent, ensure suitable system for recording that consent, including the identity of ey consented, when, to what, and what information they were provid onsent (for example, your privacy notices).

Consent has long been an importa ion law, but standards were raised significantly in 2018. It is therefore r existing consent mechanisms in light of the new requirements and, ve them.

As high as these standards are, i member the other bases for lawful processing as described above. e satisfied, it will not always be necessary to obtain consent. Fo r example, a certain amount of personal data processing will be r mance of a contract between your business and the data subject.

4.7 Special Category Data – Con

This question specifically prompts ditional "conditions for processing" where special category personal t above in the introduction to this section. Remember that you nee e conditions as well as having a lawful basis if you are processing onal data. You may also need to identify and meet additional safegu Protection Act 2018.

SAMPLE

Part 5. Fairness and Data

5.1 and 5.2 Identifying Data

Keeping in mind the purposes for [illegible] and processing of personal data, records should be kept which deta[illegible]data collected for those purposes. The information provided in this pa[illegible]ortant for a number of subsequent questions which will assess whet[illegible] is being held for lawful purposes and otherwise in compliance with [illegible]

5.3 Collecting Personal Data

Also useful in determining whethe[illegible]f personal data is appropriate and lawful is information concerning th[illegible]llection as this will have a bearing on the appropriate means of obtai[illegible]essary) and providing the required information to data subjects about [illegible]gations.

5.4 The Rights of Data Subjects

This is one of the most important[illegible]otection Legislation as compliance with these rights is vital to ensure [illegible]bjects when it comes to the use of their personal data. Under Chapt[illegible] data subjects have the following rights:

The Right to be Informed

The information you provide to [illegible]clude a range of details. Such information will often be provided[illegible]ent or similar documentation. The information that must be provided[illegible]n whether you have obtained the data from the data subject directly[illegible]tained it from a third party:

Information	Ob[illegible]	Obtained from Third Party
Identity and contact details of the data controller, the controller's representative (where applicable) and the contact details of the data controller's DPO (where applicable).	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" transfers and safeguards in place.	Yes	Yes
How long the data will be retained (or the criteria to	Yes	Yes

SAMPLE

determine how long).			
The details of data subjects' rights.	Ye		Yes
The data subject's right to withdraw consent (where applicable).	Ye		Yes
The data subject's right to complain to the ICO.	Ye		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.	Ye		No
The existence of any automated decision-making (including profiling) with details of how the decisions are made, their significance, and the consequences.	Ye		Yes

This information should be provi onal data is obtained if it is being obtained directly from the data s from a third party, the information must be provided to the data su e time (not more than one month); when communicating with the da s being used to communicate with them); or, if the data is to be disc party, before that disclosure takes place.

The Right of Access

Data subjects have the right t al data held by you along with supplementary information. In re wn as a Subject Access Request ("SAR") you must provide confirm is being processed; access to the personal data you hold on the da upplementary information (in broad terms, the same information you v vide in a privacy statement).

Under the old 1998 Data Protecti e to charge a fee for complying with SARs - usually £10 - however th AR responses to be free of charge unless the request is "manifestly " in which case a "reasonable fee" can be charged. Further copies of n also be charged for.

You should generally respond to month after receipt. In the case of complex and numerous requests, up to two months.

The Right to Rectification

Personal data should be accurat e Part 7 below). If a data subject requests the rectification of any p out them, this must be done within one month of their request. If th his can be extended by up to two

SAMPLE

months.

If the personal data in question [illegible] any third parties, the data subject should be informed of this.

The Right to Erasure

This is also known as the "right t[illegible] an unqualified right, but in broad terms, data subjects have the rig[illegible]n or destruction of personal data unless there is a sound reason for [illegible].

The most obvious way of exercisi[illegible] subject to withdraw their consent to your use of their personal dat[illegible]ng so (and there is no overriding legitimate interest that justifies cor[illegible]nces are:

- When it is no longer neces[illegible]l data with respect to the purpose for which it was originally c[illegible] also see Part 10 below);
- The personal data has bee[illegible]
- The personal data has to b[illegible]a legal obligation;
- The data is processed in re[illegible]rmation society services to a child (e.g. a social media acco[illegible]r the age of 18) (Also note that additional requirements ap[illegible] data).

There are some circumstances in [illegible]erase personal data:

- When exercising the huma[illegible]ression and information;
- In order to comply with a le[illegible]rformance of a public interest task or the exercise of official au[illegible]
- For public health purposes[illegible]erest;
- For archiving purposes th[illegible]rest, scientific research, historical research, or statistical purp[illegible]
- For the exercise or defence[illegible]

If any personal data affected by a[illegible]s been disclosed to a third party, that third party must also be inform[illegible]ss it is impossible or would require disproportionate effort to do so).

The Right to Restrict Processing

If a data subject asserts this right,[illegible]onal data, but must not process it. In practice, this may require retai[illegible]n about the data subject so as to ensure that the restriction is respe[illegible]

The right to restrict processing app[illegible]mstances:

- If a data subject has inf[illegible]al data you hold about them is inaccurate, processing of t[illegible]ted until its accuracy is verified;
- If a data subject objects to[illegible]onal data and you are considering whether your business's le[illegible]cessing that data override the data subject's interests (this a[illegible] processing is necessary for the performance of a public int[illegible]gitimate interests);
- Where the processing is u[illegible]erasure, the data subject requests restriction; or
- Where you no longer requ[illegible]ut the data subject requires it to

SAMPLE

establish, exercise, or defe

If any personal data affected by s en disclosed to a third party, that third party must also be informed it is impossible or would require disproportionate effort to do so).

The Right to Data Portability

Data subjects have the right to obt nal data from a data controller in a commonly-used format and to hav erent data controller. This enables data subjects to easily re-use the different services. As with many other rights, however, this one is n to data portability applies only:

- To personal data provided ct;
- Where the personal data is with the data subject's consent or for the performance of a co
- Where the processing of th d out by automated means.

Your business must respond to re ity within one month. This can be extended by up to two months wh lex or if you receive a number of requests.

The Right to Object

Data subjects have the right to o their personal data and must be informed of the right clearly, explic other information:

Processing based on legitimate rmance of a task in the public interest or the exercise of offici rofiling)

Under this heading, data proces you can demonstrate compelling legitimate grounds to continue wh , rights, and freedoms of the data subject. Alternatively you may cor s necessary for the establishment, exercise, or defence of legal claim

Direct marketing (including prof

There are no exceptions under thi an objection to processing for this reason, you must cease straight a

Processing for the purposes of esearch and statistics

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

Automated Decision Making Rig)

Improvements in technology ha al of data processing, including decision-making, to be automated egislation includes rights to protect data subjects against the risk of hat may harm them in some way without human intervention.

It is important to identify what, if n-making takes place within your business and in particular, evaluat nding that decision-making.

SAMPLE

Data subjects have the right, und Legislation, *not* to be subject to a decision if:

- The decision is based on a d
- The decision has a legal (o ect on the data subject.

Your procedures must ensure that o obtain human intervention in the decision-making process, able t of view, and able to obtain an explanation of the decision that ha lenge it.

The right is not unqualified, howe s if the automated decision has a legal (or similarly significant) effec urther, if the decision is necessary for the performance of a contract b a subject (or for entering into such a contract); or is authorised by bject's explicit consent has been obtained, the right also does not a

Profiling is any form of automate o evaluate personal aspects of a data subject such as may be used

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

Processing for such purposes mu ent. Suitable procedures must be used to carry out the profiling, with nd organisation measures adopted to minimise (and correct where ne he personal data used for profiling must be secured in a manner pro osed to the interests and rights of the data subjects concerned (this i mination).

Additional restrictions apply unde gislation where the personal data concerns a child or are based on s

5.5 Transfer of Personal Data

There are many reasons why yo r personal data to third parties. If your business determines the purp rocessing data and the method(s) of doing so, it will be classed as e to whom data is transferred will generally be processors, so called *ssing* data on your behalf. The UK GDPR applies to both data control .

Data controllers should, under t se data processors that provide sufficient guarantees to impleme and organisational measures in such a manner that processing wi of the Data Protection Legislation and ensure the protection of the r n short, you must ensure that any third parties to whom you transfer omplying with the law.

The UK GDPR also places restrict ty to sub-contract their work. Data processors must obtain written co ers before passing personal data

SAMPLE

onto another party themselves.

A contract should be in place be and any processor they appoint. Such contracts must include the fo

- The subject matter and the ng;
- The nature of the processi
- The type of personal data t categories of data subject; and
- The rights and obligations

As a guide, contracts between c a processors should contain the following requirements:

- The processor acts only o of the controller (unless required by law to act without);
- The processor ensures tha personal data are subject to duties of confidentiality;
- The processor takes suitab at the data is processed securely;
- The processor may not r without the controller's written consent, and then not witho lace with the sub-contractor;
- The processor must assis necessary, in handling SARs and otherwise allowing data su ghts;
- The processor must assis ng its obligations under the Data Protection Legislation with IAs, and the notification of data breaches;
- At the end of the contract, te and/or return (as requested) all personal data; and
- The processor must comp spections that the controller may carry out, provide the cont nformation required to ensure that both parties are meeting t e Data Protection Legislation, and inform the controller imm or is asked to do anything that infringes the Data Protectio plicable laws.

When conducting the data protect ensure that your business keeps track of all personal data that has rd parties (and indeed which third party or parties it has been transf ermore, ensure that data subjects are made aware of any third party personal data may be subject.

SAMPLE

Part 6. Adequacy and Rel

The third key data protection pri nal data collected and processed must be adequate and relevant in s) for which it is used. This is also known as the “minimisation princip

6.1 Assessing Adequacy and Re

When addressing the adequacy a l data collected and processed by the business, it is important to you are collecting, holding, and processing is absolutely necessa purpose(s) for which you have collected it and, most importantly, data subjects have been informed you are using it.

On the other hand, it may be that y ent data for the stated purpose(s), in which case the data protection need to change the data that you collect.

Finally, consider carefully whethe that you have. As processes and procedures within your business ou are still collecting and holding personal data that is no longer r any type(s) of personal data are identified under this heading, thes herwise disposed of and collection should also cease.

6.2 Reviewing Data and Method

Having assessed the current sta held by your business, it is also important to assess the procedu ing that data for adequacy and relevance on a regular basis. Co n reviews should be, and whether they should be prompted by other ojects utilising personal data.

SAMPLE

Part 7. Accuracy

Accuracy forms the basis of the principle. Personal data must be accurate and, where necessary, , every reasonable step must be taken to ensure that any person te is corrected or erased without delay. Reasonable steps should to ensure that data is accurate at the time of collection, whether fr or from third parties, as well as steps to maintain the accuracy of t

7.1 Collecting Accurate Data an

This section of the audit identifies o ensure the accuracy of personal data collected and held by the bus g what steps are taken at the time of collection to ensure accuracy, asures in place to keep the data accurate. Consider the type(s) of whether they are likely to change. Addresses and other contact info er time, as may certain personal circumstances. Consider how yo ese changes. In some cases, for example, it may be appropriate to once a year asking them to check, confirm, and/or update their perso m.

7.2 Accuracy of Data Transferre

It is important to maintain the accu s been transferred to a third party processor. In addition to evaluatin cking the accuracy of data prior to transfer, consider also how that ac r the transfer.

SAMPLE

Part 8. Data Transfers Ab

Transferring data to recipients loc enerally much simpler from a data protection perspective than transfe ed in a country outside of the UK. As of 1 January 2021, transfers to EA from the UK will continue to be permitted as they were prior to th sition period. Moreover, under the terms of the EU-UK Trade and C EEA to UK transfers will also be permitted (during a temporary pe uacy decision – see below), thus laying to rest widespread concer uld require additional safeguards, such as standard contractual claus .

It should be noted in this context th electronic access across borders.

If your business wishes to trans nd these areas, however, things become more complicated. Perso nsferred if the destination country, territory, or one or more specifi country (or, if the recipient is an international organisation, that ace an adequate level of data protection or if certain other condit

Under the EU GDPR regime, tra to third countries were permitted under adequacy decisions reac Commission or under the other appropriate safeguards set out d of the Brexit transition period, transitional provisions will ensure dequacy decisions and approved safeguards continue to be recogn will also be able to make its own adequacy decisions ("adequacy r e further safeguards following the end of the Brexit transition period.

Under the terms of the EU-UK T Agreement, reached between the European Commission and the U 0, transfers of personal data from the EEA to the UK will be permitte x months. This so-called "specified period" is designed to maintain d he European Commission time to adopt an adequacy decision in re hich, data flows should be able to continue without the transitional pr

The trade agreement does, howe tions on the UK in exchange for allowing data flows to continue ***d eriod***. Changes to the UK's data protection legislation cannot be m . Similarly, the exercise of certain "designated powers" (including th ts own adequacy regulations and approve its own safeguards) are s ing the specified period.

8.1 and 8.2 Destination Country ws

Begin by identifying the country e recipients of personal data are located. If any recipient is in a no EA country, the first step will be to determine whether or not that cou more specified sectors within that country (or the international or ensures an adequate level of protection.

8.3 Alternative Conditions

The "other conditions" referred to a

- You have the explicit and i ata subject to the transfer; or
- The transfer is necessary f contract between you and the data subject or for pre-contractu a subject's request; or

SAMPLE

- The transfer is necessary … contract made in the interests of the data subject between y…
- The transfer is necessary f… st reasons; or
- The transfer is necessary f… ercise, or defence of legal claims; or
- The transfer is necessary … rests of the data subject or other persons, where the data su… ally unable to give consent; or
- The transfer is made from… r the law, is intended to provide information to the public (… consultation either by the general public or by those able to s… in inspecting the register).

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

- An agreement between pul… or
- Binding corporate rules; or
- Standard data protection c… e European Commission (prior to the end of the Brexit transit… or
- Standard data protection c… lations made by the Secretary of State (subject to temporary… or
- Standard data protection cl… ICO (see above); or
- Compliance with an approv…
- Certification under an appr… e as provided for in the UK GDPR; or
- Contract clauses agreed a… ; or
- Provisions in administrative… public authorities or other bodies authorised by the ICO.

If none of the above can be satisfi… ows one-off or infrequent transfers of personal data which concern … of data subjects in the following circumstances, provided the ICO i… ed data subjects are provided with additional information:

- The transfer is not being m… exercising its public powers;
- The transfer is not repetitiv…
- The personal data being tra… a limited number of data subjects;
- The transfer is necessary … mate interests of the organisation transferring the data, as lo… not overridden by the interests of the data subject(s); and
- Having assessed all circun… e transfer, suitable safeguards are in place by the transfe… rotect the personal data being transferred.

8.4 Checking Compliance

Regardless of which of the above … transfers is being relied upon, it is advisable to take steps to ensure … tions are being complied with on a regular basis. Consider whether … conduct data protection audits of data processors located in third co… you have a point of contact within any recipient organisation that can… ompliance.

SAMPLE

Part 9. Record Keeping

Keeping track of the personal data… cessed by your business is vital in order to ensure full compliance wi… s laid down by the Data Protection Legislation. In particular, if your … n 250 employees, the UK GDPR imposes specific record-keeping re…

9.1 and 9.2 Record Keeping Req…

Since the nature of records requir… part by the size of your business, start this section by determining … loyees. If the business has more than 250 employees, the UK GDP… records that include the following details:

- The name and details of yo…
- The name and details of ot… plicable;
- The name and details of yo… ta protection officer, if applicable;
- The purpose(s) for which y… ersonal data;
- The type(s) of personal dat… ed;
- The type(s) of data subject… and processed;
- The recipient(s) of persona…
- Details of any transfers of… recipients in third countries (see Part 8) including any and a… eguards in place;
- Personal data retention sch…
- Where possible, details of … ational security measures in place to protect personal data (se…

If the business has less than 25… required only to keep records of personal data processing that may… ", for example:

- Personal data processing t… to the rights and freedoms of data subjects; or
- Processing sensitive pers… oncerning criminal offences and convictions.

Further documentation recommen… onstrate compliance with the Data Protection Legislation includes:

- Information required for p… vacy information", "privacy policy" etc);
- Records of consent;
- Contracts with data proces…
- The location of personal da…
- Reports of Data Protection …
- Records of personal data b…
- Information required for th… category personal data or criminal offence data under the Dat…

SAMPLE

Part 10. Data Retention a

Personal data must be kept in a f entification of data subjects for no longer than is necessary for the e personal data is collected and processed.

The Data Protection Legislation a to be stored for longer periods where the data will be processed poses in the public interest, or for scientific or historical research pu rposes subject to the requirement that technical and organisational ce to ensure the respect for the principle of data minimisation. Exa provided in the UK GDPR include pseudonymisation (provided that t e data is retained can be fulfilled). Where the purposes can be fulfi ng which does not enable (or no longer enables) the data subject to ses should be fulfilled in that way.

In short, your business should n that enables data subjects to be identified for any longer than ne reasons for which you originally collected it.

10.1 Data Retention

In this section, refer back to the lis) collected and processed by your business, and the purpose(s) for d and processed. In each case, it should be established how the ret ed, with such methods reviewed if necessary. It is also important tha ecorded which will help to ensure that no personal data is kept for ar .

10.2 Reviewing Data Retention

While all retention periods should any personal data is collected or processed, it is good practice to r ods from time to time, even if the purposes for, and methods of, pro

10.3 Deletion of Personal Data

Personal data must be securely d hen it is no longer necessary, or when a data subject exercises the

If the data is stored electronically s of secure deletion are available. Some secure deletion methods, he data after deleting it, thereby reducing the likelihood that it can lest form of this merely overwrites the data with zeros in a single pas s overwrite the data multiple times with randomised data. The greate tes, the more secure the deletion will be (and the longer the deletion r, that such methods are generally more suited to traditional spinning modern solid-state storage stores data in a very different way. Sec red on solid state media typically involves encryption, although over

If the data is stored in hard copy fo osal typically include shredding or burning. Note, however, that not d equal and a basic home-office machine is not likely to render you erable. International Standard DIN 66399 specifies seven levels of se el 3 is currently recommended as a minimum level for disposing of p

10.4 Longer Retention of Data

SAMPLE

As noted above, certain circum to be retained for longer. The requirements can be complex, but articularly in the business context, is the removal of details that enab ersonally identified. It may be the case that a business needs to re figures, but those figures do not need to be associated with individu n in many cases.

10.5 Home Working

If the business has introduced ho eased it) in response to the 2020 outbreak of the novel coronavirus have an impact on your ability to ensure the secure deletion or disp the case of electronic data, it will be important to ensure that the sa normal working conditions can still be used, for example, if your staff puters and devices. In the case of physical copies of personal data, ment (e.g. a DIN 3 shredder) was taken home or remains accessible necessary visits to your premises, it may be preferable to retain the nd securely until such equipment can be used. This may involve re in question for longer than would normally be necessary; however simply tearing up the paper and disposing of it in normal household til it can be disposed of correctly is arguably a safer choice.

SAMPLE

Part 11. Data Security

The Data Protection Legislation r ata is processed in a manner that ensures appropriate security of th g protection against unauthorised or unlawful processing, and a destruction, or damage, using appropriate technical or organisati

The level of security required will te to the risks posed to the rights and freedoms of data subjects. M tions, the nature, scope, context, and purposes of data processing, f the art will also be factored into determining what is appropriate. E UK GDPR include:

- The pseudonymisation and data;
- The ability to ensure the o tegrity, availability, and reliance of processing systems and se
- The ability to restore the av ersonal data in a timely manner in the event of a physical or t
- A process for regularly t evaluating the effectiveness of technical and organisationa the security of the processing.

11.1 to 11.7 Physical Data

A great deal of emphasis is place , but a lot of personal data is still stored and processed on paper - e he security measures that apply to physical data storage are likely to e that apply to electronic storage.

Begin this section by identifying t ata that your business stored in a physical form. This will enable yo ether the answers to the following questions cover all applicable data

A range of different organisationa ace to control access to personal data stored in physical form. An such measures is the granting of different access levels to staff, e who have a legitimate need to access the data are authorised a al measures should be supported by physical measures such as loc

Keeping access logs can also a ecurity. Not only do logs help to ensure that only authorised staff g the data, but they can also be helpful in keeping track of copies an be invaluable in tracking down missing items. In addition, consid res. Backing up electronic data is comparatively straightforward an backing up physical data may require more direct action such a pies in an alternative location, or storing copies electronically.

If your business has introduced h eased it) in response to the 2020 outbreak of the novel coronavirus ave an impact on the security of physical data records. Indeed, it r existing measures and systems entirely (if temporarily) redundant. cult and more important to devise systems to keep track of physical and, as noted above in Part 10, it may be necessary to retain them y planned in order to ensure safe and secure disposal.

11.8 to 11.15 Electronic Data

SAMPLE

As with personal data stored in a tion of the audit begins again by listing data types - in this case, dat

Also as with physical data, orga important when it comes to the security of electronic data. Once of access for staff will be useful, ensuring that only those who nee onal data to perform their job role have access to it. This is genera with electronic data than it is with physical data as usernames and gured to grant access to selective areas of a computer system on a p

Usernames and passwords shoul a strong approach to IT security, and should work alongside other such as firewalls, encryption, virus and malware protection, and regul updates.

Electronic security can also be me cases with physical security measures. Server rooms, for exa at all times with access limited to those staff members with legitimat

Care must always be taken wh ff's use of computers and other electronic resources, however it ca , when used correctly, to enhance the security of personal data.

In addition to controlling access to ctronically, consider the measures that will be useful in protecting th sures such as virus and malware protection, encryption, firewalls, a d security updates are essential. Such measures should also be ve. If a user wishes to use, for example, a USB drive, it is good the drive is scanned for viruses before it can be used. Strict limita ced on staff members' use of their own personal devices.

If your business has introduced h reased it) in response to the 2020 outbreak of the novel coronavirus ave an impact on the security of electronic personal data. Ideally, y ad the time to implement security measures such as Virtual Private will issue centrally administered laptops and other devices to sta siness can maintain control over important security software, updat llation of unauthorised software. If this is not the case, however, st and processing personal data on personal devices via relatively ur with measures to protect physical data, many of your electronic sec rendered ineffective by a sudden shift to home working. Training ny-issued software, and indeed company-issued hardware (for ex set up prior to being delivered to staff at home) can help to significa

11.16 to 11.23 System Security

All computers and other electronic onal data can be accessed should be protected with username and possible. Also where possible, all users should have a unique userr e that this may not be possible in the case of, for example, Apple adOS operating system currently does not support multiple users. e should still be protected with a passcode or with biometric ID suc g of such devices should thus be limited to those staff with the same

Consider the rules and policies t and passwords. The golden rule should always apply - no sharing y reason. Even IT staff should not

SAMPLE

be privy to anyone's password. C a method of changing a forgotten password is in place that keeps Further important considerations include the security of passwords asswords be easily guessed by a human being, but the simpler the p y it can be cracked by a computer. According to howsecureismypass l "password1" would be cracked instantly by a computer. Convers mputer one trillion years to crack "2042GreenTree12!". Whether by echnical means, ensure that users are required to choose secure pas uld also be changed regularly, and many IT administrative systems al et.

Different user accounts should enable the implementation and enforcement of different access le Such access levels may need to be reviewed, for example, when a ges, or when they are assigned to a new project which requires acce ven less personal data.

Additional security measures may able to access personal data from outside your business's premises. mpany intranet site may be helpful, as are facilities such as Virtual P which provide a secure "tunnel" through which users can access th

A further key point to consider u stem security is the revocation of access to personal data when a m e business or is likely to be absent for a prolonged period of time. need to retain access to certain facilities for a period after departur that a compelling reason could be found to justify continued access t

Again, if the business has introdu as increased it) in response to the 2020 outbreak of the novel coro s will have an impact on system security, particularly if staff are u t instead of company-owned and administered devices. As above, n use, consider increased training and awareness and, if possible, l elivering properly administered IT equipment to your staff at home. es in conjunction with the "BYOD" section, below. Even if your bus ly take a BYOD approach to IT equipment, guidance and polici be particularly helpful in these circumstances.

11.24 to 11.27 Devices Provided

This section examines security m puters, laptops, and other devices such as tablets and smartphones t usiness to staff. Mobile devices in particular pose a significant hazat security of personal data as they can be far more easily lost, st ft unattended and accessible to unauthorised users when compare s that never leave the workplace.

If personal data is accessible on s portant to consider first of all what type(s) of data is accessible and necessary. The same applies to personal data that is stored on la es, although a stronger case can arguably made for access than The mere fact that data can be accessed does not necessarily r e to an unauthorised user of the device, whereas data stored is p nyone with access to the device, including someone who finds it wh

To minimise such risks, evaluat ch as encryption. If a device is encrypted, even if personal data , it will be very difficult - in some cases practically impossible - to ac e requisite access credentials.

SAMPLE

11.28 to 11.34 BYOD

Bring Your Own Device, or "BYO s. Staff members are able to use their own personal computers and While this provides convenience to staff and cost savings to your b entially serious risks where data protection is concerned.

A sound first step in ensuring se onment is to implement a BYOD policy. A properly-drafted BYOD key aspects including employee obligations, acceptable usage, and on compliance.

As with business-supplied laptops stablish whether personal data is accessible or stored on BYOD d t access or storage is absolutely necessary. Even more so than d laptop, it is arguable that the storage of personal data on a BYO bed as undesirable at best.

In addition to the security measure lace for offsite access to personal data, consider what additional me ry for BYOD devices, such as the provision of security software an s such as the use of encryption, secure passwords, the creation o e or login for work purposes, and testing and approval procedures can be used to access or store personal data. A further prudent cord of all BYOD devices in use, including details of the staff memb used, the personal data accessible and/or stored on it, the purpose(s and the data are used, and other valuable IT security information ersions and security measures implemented.

SAMPLE

Part 12. Data Breaches

The final part of the audit address table care is taken to comply with the letter and spirit of the Data P eaches should be minimal or non-existent. Nevertheless, it is impo act in the event that one occurs. Depending on the nature of a bre reported to the ICO and, in some cases, also to the data subjects af

A personal data breach is define which results in the destruction, loss, alteration, unauthorised discl ersonal data.

The first step is the internal ident n. In a small business with only a few employees, this may be easy business, the more important it is that a number of people know wha the breach may be reported to the business's DPO or other appropria kly as possible.

The ICO must be informed only result in a risk to the rights and freedoms of data subjects. If suc essed, it will be likely to have a significant detrimental effect on t bles provided by the ICO include discrimination, reputational damag ss of confidentiality. Data subjects must be informed of a breach if t ult in a *high* risk to the rights and freedoms of the data subjects.

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

When notifying the ICO, a breach the following information:

- The categories and approx bjects concerned;
- The categories and approx l data records concerned;
- The name and contact deta O (or other contact point if no DPO has been appointed);
- A description of the likely c ch; and
- Details of the measures deal with the breach including, where relevant, measures sible adverse effects.

It is important to note that failure rsonal data breach can result in a significant fine of up to £8.7m or 2 l turnover.

SAMPLE