**PREPARING FOR THE**

**GENERAL DATA PROTECTION REGULATION (GDPR)**

**INDEX**

**TOPIC PAGE No.**

**Introduction 2**

**Making Everyone Aware 4**

**Holding Information 5**

**The Rights of Individuals 7**

**Requests for Access 10**

**Privacy and Processing Protocols 11**

**Obtaining Consent 12**

**Children 14**

**Breaches of Data Law 15**

**Design & Impact Assessments 17**

**Data Protection Officer 18**

**Exemptions (Derogations) 20**

**Checklist 1 – Lawful basis for processing data 21**

**Checklist 2 – Questions to ask when deciding if processing is appropriate 22**

**Checklist 3 – Asking for, recording and managing consent 23**

**Checklist 4 – Legitimate interests 25**

**Checklist 5 – Automated individual decision-making and profiling 26**

**Checklist 6 – Controller and Processor contracts 28**

**Checklist 7 – Documentation 31**

**Notes 33**

**INTRODUCTION**

The new law comes in to force on 25th May 2018. It will replace the 1998 Data Protection Act – and it will affect all of us. As with most new laws the GDPR contains lots of legal and technical jargon, which many people find confusing. Our workshop is designed to examine and explain what it means in practice for business owners, staff and other stakeholders. Our emphasis is on understanding the core requirements and practical implementation of the GDPR – and what you and your people must know and do.

Many parts of the GDPR are the same or similar to those in the current Data Protection Act (DPA – 1998). If you are abiding by the current law, many things that you do now will form the bedrock of the new GDPR and will be a good starting point from which to build. However, under GDPR, there are some new elements and quite significant enhancements, so you’ll have to do some things differently and others for the first time.

It’s essential to plan your approach to GDPR compliance now and to get ‘buy in’ from relevant key people both inside and outside your organisation. You may need, for example, to put new procedures in place to deal with the GDPR’s new transparency and individuals’ rights provisions. In a large or complex business this

could have significant budgetary, IT, personnel, governance and communications implications. For smaller organisations the implications may be easier to interpret and quantify – but you’ll still need to comply in every aspect.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas covered in the workshop and these notes will require organisations to review their approach to governance and how they manage data protection as a corporate issue. For instance, one aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

It’s important not to feel daunted by all of this. As you work through the key sections you may be pleasantly surprised by how much you have in place already – and, by the end of the workshop, you will have a clear understanding of what more you need to do and a clear pathway template on how to achieve it.

The workshop’s ten top topics are:

1. **Making Everyone Aware** – Ensuring that all business owners, managers, staff and stakeholders know about the new law.
2. **Holding Information** – Knowing what personal data you hold, why you have it and who can have access; also, what are the legal methods of communication
3. **The Rights of Individuals** – Checking/creating your processes and procedures to ensure you know what data you’re allowed to hold, how it’s held and when to delete it
4. **Requests for Access** – How to handle requests from different sources; what you’re allowed to share and what you’re not
5. **Privacy and Processing Protocols** – Helping you to identify the legal basis on which you process data and updating your published policies
6. **Obtaining Consent** – Ensuring you review how to seek, record and manage consent – and updating methods and processes as appropriate
7. **Children** – If you hold data on children, making sure you can legally verify ages – and update consent data from responsible adults
8. **Breaches of Data Law** – Checking that you have procedures in place to detect, report and investigate potential or alleged breaches
9. **Design & Impact Assessments** – Understanding and complying with the International Commissioner’s Office codes of practice and guidelines
10. **Data Protection Officer** – Formal or informal, it’s best practice to nominate an individual to take responsibility for data protection compliance in your organisation

We will have some group activities and analysis to aid understanding and there will also be a Q & A session so you can raise any matters that you believe are unique to your organisation or on which you want further guidance.

**1. Making Everyone Aware** – Ensuring that all business owners, managers, staff and stakeholders know about the new law.

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation’s risk register, if you have one. Implementing the GDPR could have significant resource implications,

especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

It will be a good idea to hold meetings/briefings for your people so you can tell them, in terms appropriate to their job activities, what the GDPR is all about – and it may well be helpful to use some of our checklists for this exercise.

Please don’t forget other stakeholders who may not be your direct full and/or part-time employees. For instance, you may use temps, ‘bank’ staff (people already known to you who you employ intermittently on a temporary basis), consultants, contractors and third-party employees on secondments. In addition, you need to review what information you hold and share and which of the above have access to it (or add to it). It may be useful to give all or some of these people a copy of these workshop notes and, if appropriate, some of the documents that you can download from our website.

The key message here is: ‘don’t assume’. You need to be absolutely sure that all relevant people connected to and with your organisation are fully up to speed with the provisions of the GDPR as it affects the activities they undertake on behalf of your organisation.

**2. Holding Information** – Knowing what personal data you hold, why you have it and who can have access; also, what are the legal methods of communication

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas. The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won’t be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR’s accountability principle, which requires organisations to be able to show how they comply with the data protection principles; for example, by having effective policies and procedures in place.

It will be helpful at this point to give some examples of ‘information’ in this context:

* **Personal data**

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

* **Sensitive personal data**

The GDPR refers to sensitive personal data as “special categories of personal data”

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing – just as you would apply now with, for instance, DBS checks and information you may hold about convictions which become ‘spent’ after you have made the initial recording of the information.

This is what the GDPR says about the ‘lawful basis’ on which you hold information:

* You must have a valid lawful basis in order to process personal data.
* There are six available lawful bases for processing. No single basis is ’better’ or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

1. Most lawful bases require that processing is ‘necessary’. If you can reasonably achieve the same purpose without the processing, you won’t have a lawful basis.
2. You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.
3. Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
4. If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
5. If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
6. If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

**3. The Rights of Individuals** – Checking/creating your processes and procedures to ensure you know what data you’re allowed to hold, how it’s held and when to delete it.

You should review your current privacy notices and put a plan in place for making any necessary changes by 25th May 2018.

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the Information Commissioner’s Office (ICO) if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

* the right to be informed;
* the right of access;
* the right to rectification;
* the right to erasure;
* the right to restrict processing;
* the right to data portability;
* the right to object; and
* the right not to be subject to automated decision-making, including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

* to personal data an individual has provided to a controller;
* where the processing is based on the individual’s consent or for the

performance of a contract; and

* when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine readable form and provide the information free of charge.

Here is what the GDPR says about the lawful basis on which you are allowed to process personal data:

**(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

**(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

**(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

**(d) Vital interests:** the processing is necessary to protect someone’s life.

**(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

When preparing to process personal data, consider the following questions:

* What is your purpose – what are you trying to achieve?
* Could you reasonably achieve it in a different way?
* Do you have a choice over whether or not to process their data?

If you are considering processing someone’s data – apart from legal obligation, contract, vital interests or public task, you need to consider the wider context in which you are proposing to collect the data. To this end, you should ask yourself the following questions:

* Who does the processing benefit?
* Would individuals expect this processing to take place?
* What is your relationship with the individual?
* Are you in a position of power over them?
* What is the impact of the processing on the individual?
* Are they vulnerable?
* Are some of the individuals concerned likely to object?
* Are you able to stop the processing at any time on request?

**4. Requests for Access** – How to handle requests from different sources; what you’re allowed to share and what you’re not

Firstly, you need to establish if the person or individual requesting access to data that you hold has a legal right to receive that data. In Section 3 of these notes we listed some ‘lawful bases’ on consent and it would be worthwhile reviewing these in the context of this current section too.

Essentially, you need to consider if the requestor has the legal right to the data that you hold

* If you are in doubt, ask them to provide/explain their legal authority
* If mixed data, do you need additional consent from the individual concerned?
* If the request is from the individual concerned, and it’s about them alone, the Section 3 rules apply

You should update your procedures and plan how you will handle requests to take account of the new rules:

* In most cases you will not be able to charge for complying with a request.
* You will have a month to comply, rather than the current 40 days.
* You can refuse or charge for requests that are manifestly unfounded or excessive.
* If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online – but, if you implement this, do make sure that they can only access their own data, not anyone else’s!

**5. Privacy and Processing Protocols** – Helping you to identify the legal basis on which you process data and updating your published policies.

You should identify the lawful basis for your processing activity and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals’ rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to help you comply with the GDPR’s ‘accountability’ requirements.

**6. Obtaining Consent** – Ensuring you review how to seek, record and manage consent – and updating methods and processes as appropriate

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don’t meet the GDPR standard.

You may wish read the detailed guidance the ICO has published on consent under the GDPR, which is available to download from our website; however, for most workshop attendee organisations, it is likely that these notes – together with our checklist at the end of this document – will suffice.

Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.

You are not required to automatically ‘repaper’ or refresh all existing DPA consents in preparation for the GDPR; however, if you rely on individuals’ consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

To help you better understand the context of ‘consent’, here are some points to consider:

* The GDPR sets a high standard for consent. But you often won’t need consent. If consent is difficult, look for a different lawful basis.
* Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement, and enhance your reputation.
* Check your consent practices and your existing consents. Refresh your consents if they don’t meet the GDPR standard.
* Consent requires a positive opt-in. Don’t use pre-ticked boxes or any other method of default consent.
* Explicit consent requires a very clear and specific statement of consent.
* Keep your consent requests separate from other terms and conditions.
* Be specific and ‘granular’ so that you get separate consent for separate things. Vague or blanket consent is not enough.
* Be clear and concise.
* Name any third party controllers who will rely on the consent.
* Make it easy for people to withdraw consent and tell them how.
* Keep evidence of consent – who, when, how, and what you told people.
* Keep consent under review, and refresh it if anything changes.
* Avoid making consent to processing a precondition of a service.
* Public authorities and employers will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.

**7. Children** – If you hold data on children, making sure you can legally verify ages – and update consent data from responsible adults

You should start thinking now about whether you need to put systems in place to verify individuals’ ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children’s personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services (‘information society services’) to children and relies on consent to collect information about them, then you may need a parent or guardian’s consent in order to process their personal data lawfully. ‘Information society services’ includes most internet services provided at the user’s request, normally for remuneration. The GDPR emphasises that protection is particularly significant where children’s personal information is used for the purposes of marketing and creating online profiles.

The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding ‘parental responsibility’.

This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children’s data your privacy notice must be written in language that children will understand.

Further public consultation on potential amendments/additions to GDPR provisions relating to children closes on 28th February 2018 – but no date has yet been set for publication of the subsequent report or, indeed, a date for any implementation/s. We will seek to advise all workshop attendees once the information is available.

**8. Breaches of Data Law** – Checking that you have procedures in place to detect, report and investigate potential or alleged breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Here’s an example of a potential breach:

A care home could be responsible for a personal data breach if a patient’s health record is inappropriately accessed due to a lack of appropriate internal controls.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals.

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of client/customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases. A ‘high risk’ means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay. Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

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

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

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

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Further amendments may be made to GDPR rules on data breaches, which the IPO expect to publish “in early 2018” – we’ll let you know once we receive this additional information.

**9. Design & Impact Assessments** – Understanding and complying with the International Commissioner’s Office codes of practice and guidelines

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term ‘data protection by design and by default’. It also makes PIAs – referred to as ‘Data Protection Impact Assessments’ or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in

high risk to individuals, for example:

* where a new technology is being deployed;
* where a profiling operation is likely to significantly affect individuals; or
* where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

It would also be a good idea familiarise yourself now with the guidance the ICO has produced on PIAs as well as guidance from the Article 29 Working Party, and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management. This guidance document is available on our website.

**10. Data Protection Officer** – Formal or informal, it’s best practice to nominate an individual to take responsibility for data protection compliance in your organisation

The GDPR makes it a requirement that organisations appoint a data protection officer (DPO) in some circumstances – but we recommend that every organisation appoints one. The GDPR also contains provisions about the tasks a DPO should carry out and the duties of the employer in respect of the DPO. The rules say that a DPO must be appointed if you:

* are a public authority (except for courts acting in their judicial capacity);
* carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
* carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size.

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

The DPO’s minimum tasks are defined in Article 39:

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

You must ensure that:

* The DPO reports to the highest management level of your organisation – i.e. board level. The DPO operates independently and is not dismissed or penalised for performing their task.
* Adequate resources are provided to enable DPOs to meet their GDPR obligations.

You can allocate the role of DPO to an existing employee as long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. You can also contract out the role of DPO externally.

The GDPR does not specify the precise credentials a data protection officer is expected to have, although it does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

**EXEMPTIONS (DEROGATIONS)**

Article 23 enables Member States to introduce derogations to the GDPR in certain situations. Member States can introduce exemptions from the GDPR’s transparency obligations and individual rights, but only where the restriction respects the essence of the individual’s fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

* national security;
* defence;
* public security;
* the prevention, investigation, detection or prosecution of criminal offences;
* other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
* the protection of judicial independence and proceedings;
* breaches of ethics in regulated professions;
* monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
* the protection of the individual, or the rights and freedoms of others; or
* the enforcement of civil law matters.

Chapter IX provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities. These include processing that relates to:

* freedom of expression and freedom of information;
* public access to official documents;
* national identification numbers;
* processing of employee data;
* processing for archiving purposes and for scientific or historical research and statistical purposes;
* secrecy obligations; and
* churches and religious associations.

Please ask us for focussed guidance if your organisation and/or its activities fall under any of these exemptions/derogations.

**CHECKLIST 1 – Lawful basis for processing data**

☐ We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity.

☐ We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.

☐ We have documented our decision on which lawful basis applies to help us demonstrate compliance.

☐ We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.

☐ Where we process special category data, we have also identified a condition for processing special category data, and have documented this.

☐ Where we process criminal offence data, we have also identified a condition for processing this data, and have documented this.

**CHECKLIST 2 – Questions to ask when deciding if processing is appropriate**

If you are processing for purposes other than legal obligation, contract, vital interests or public task, then the appropriate lawful basis may not be so clear cut. In many cases you are likely to have a choice between using legitimate interests or consent. You need to give some thought to the wider context, including:

* Who does the processing benefit?
* Would individuals expect this processing to take place?
* What is your relationship with the individual?
* Are you in a position of power over them?
* What is the impact of the processing on the individual?
* Are they vulnerable?
* Are some of the individuals concerned likely to object?
* Are you able to stop the processing at any time on request?

You may prefer to consider legitimate interests as your lawful basis if you wish to keep control over the processing and take responsibility for demonstrating that it is in line with people’s reasonable expectations and wouldn’t have an unwarranted impact on them. On the other hand, if you prefer to give individuals full control over and responsibility for their data (including the ability to change their mind as to whether it can continue to be processed), you may want to consider relying on individuals’ consent.

**CHECKLIST 3 – Asking for, recording and managing consent**

☐ We have checked that consent is the most appropriate lawful basis for processing.

☐ We have made the request for consent prominent and separate from our terms and conditions.

☐ We ask people to positively opt in.

☐ We don’t use pre-ticked boxes or any other type of default consent.

☐ We use clear, plain language that is easy to understand.

☐ We specify why we want the data and what we’re going to do with it.

☐ We give individual (‘granular’) options to consent separately to different purposes and types of processing.

☐ We name our organisation and any third party controllers who will be relying on the consent.

☐ We tell individuals they can withdraw their consent.

☐ We ensure that individuals can refuse to consent without detriment.

☐ We avoid making consent a precondition of a service.

☐ If we offer online services directly to children, we only seek consent if we have

age-verification measures (and parental-consent measures for younger children) in place.

☐ We keep a record of when and how we got consent from the individual.

☐ We keep a record of exactly what they were told at the time.

☐ We regularly review consents to check that the relationship, the processing and the purposes have not changed.

☐ We have processes in place to refresh consent at appropriate intervals, including any parental consents.

☐ We consider using privacy dashboards or other preference-management tools as a matter of good practice.

☐ We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.

☐ We act on withdrawals of consent as soon as we can.

☐ We don’t penalise individuals who wish to withdraw consent.

**CHECKLIST 4 – Legitimate interests**

☐ We have checked that legitimate interests is the most appropriate basis.

☐ We understand our responsibility to protect the individual’s interests.

☐ We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.

☐ We have identified the relevant legitimate interests.

☐ We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

☐ We have done a balancing test, and are confident that the individual’s interests do not override those legitimate interests.

☐ We only use individuals’ data in ways they would reasonably expect, unless we have a very good reason.

☐ We are not using people’s data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.

☐ If we process children’s data, we take extra care to make sure we protect their interests.

☐ We have considered safeguards to reduce the impact where possible.

☐ We have considered whether we can offer an opt out.

☐ If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.

☐ We keep our LIA under review, and repeat it if circumstances change.

☐ We include information about our legitimate interests in our privacy notice.

**CHECKLIST 5 – Automated individual decision-making and profiling**

To comply with the GDPR...

☐ We have a lawful basis to carry out profiling and/or automated decision-making and document this in our data protection policy.

☐ We send individuals a link to our privacy statement when we have obtained their personal data indirectly.

☐ We explain how people can access details of the information we used to create their profile.

☐ We tell people who provide us with their personal data how they can object to profiling, including profiling for marketing purposes.

☐ We have procedures for customers to access the personal data input into the profiles so they can review and edit for any accuracy issues.

☐ We have additional checks in place for our profiling/automated decision-making systems to protect any vulnerable groups (including children).

☐ We only collect the minimum amount of data needed and have a clear retention policy for the profiles we create.

As a model of best practice...

☐ We carry out a DPIA to consider and address the risks before we start any new automated decision-making or profiling.

☐ We tell our clients/customers about the profiling and automated decision-making we carry out, what information we use to create the profiles and where we get this information from.

☐ We use anonymised data in our profiling activities.

To comply with the GDPR...

☐ We carry out a DPIA to identify the risks to individuals, show how we are going to deal with them and what measures we have in place to meet GDPR requirements.

☐ We carry out processing under Article 22(1) for contractual purposes and we can demonstrate why it’s necessary.

OR

☐ We carry out processing under Article 22(1) because we have the individual’s explicit consent recorded. We can show when and how we obtained consent. We tell individuals how they can withdraw consent and have a simple way for them to do this.

OR

☐ We carry out processing under Article 22(1) because we are authorised or required to do so. This is the most appropriate way to achieve our aims.

☐ We don’t use special category data in our automated decision-making systems unless we have a lawful basis to do so, and we can demonstrate what that basis is. We delete any special category data accidentally created.

☐ We explain that we use automated decision-making processes, including profiling. We explain what information we use, why we use it and what the effects might be.

☐ We have a simple way for people to ask us to reconsider an automated decision.

☐ We have identified staff in our organisation who are authorised to carry out reviews and change decisions.

☐ We regularly check our systems for accuracy and bias and feed any changes back into the design process.

As a model of best practice...

☐ We use visuals to explain what information we collect/use and why this is relevant to the process.

☐ We have signed up to [standard] a set of ethical principles to build trust with our customers. This is available on our website and on paper.

**CHECKLIST 6 – Controller and Processor contracts**

Our contracts include the following compulsory details:

☐ the subject matter and duration of the processing;

☐ the nature and purpose of the processing;

☐ the type of personal data and categories of data subject; and

☐ the obligations and rights of the controller.

Our contracts include the following compulsory terms:

☐ the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);

☐ the processor must ensure that people processing the data are subject to a duty of confidence;

☐ the processor must take appropriate measures to ensure the security of processing;

☐ the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;

☐ the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

☐ the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

☐ the processor must delete or return all personal data to the controller as requested at the end of the contract; and

☐ the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

As a matter of good practice, our contracts:

☐ state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and

☐ reflect any indemnity that has been agreed.

The Processor must:

☐ only act on the written instructions of the controller (Article 29);

☐ not use a sub-processor without the prior written authorisation of the controller (Article 28.2);

☐ co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;

☐ ensure the security of its processing in accordance with Article 32;

☐ keep records of its processing activities in accordance with Article 30.2;

☐ notify any personal data breaches to the controller in accordance with Article 33;

☐ employ a data protection officer if required in accordance with Article 37; and

☐ appoint (in writing) a representative within the European Union if required in accordance with Article 27.

A Processor should also be aware that:

☐ it may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR;

☐ if it fails to meet its obligations, it may be subject to an administrative fine under Article 83 of the GDPR;

☐ if it fails to meet its GDPR obligations it may be subject to a penalty under Article 84 of the GDPR; and

☐ if it fails to meet its GDPR obligations it may have to pay compensation under Article 82 of the GDPR.

**CHECKLIST 7 – Documentation**

Documentation of processing activities – requirements:

☐ If we are a controller for the personal data we process, we document all the applicable information under Article 30(1) of the GDPR.

☐ If we are a processor for the personal data we process, we document all the applicable information under Article 30(2) of the GDPR.

If we process special category or criminal conviction and offence data, we document:

☐ the condition for processing we rely on in the Data Protection Bill;

☐ the lawful basis for our processing; and

☐ whether we retain and erase the personal data in accordance with our policy document.

☐ We document our processing activities in writing.

☐ We document our processing activities in a granular way with meaningful links between the different pieces of information.

☐ We conduct regular reviews of the personal data we process and update our documentation accordingly.

Documentation of processing activities – best practice

When preparing to document our processing activities we:

☐ do information audits to find out what personal data our organisation holds;

☐ distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and

☐ review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

☐ information required for privacy notices;

☐ records of consent;

☐ controller-processor contracts;

☐ the location of personal data;

☐ Data Protection Impact Assessment reports; and

☐ records of personal data breaches.

☐ We document our processing activities in electronic form so we can add, remove and amend information easily.

**NOTES**

**NOTES**