**GDPR Self-Assessment Template and Checklist**

**Contents**

The New Regulations

The right to data protection

Data protection roles, rights and obligations

What is personal data?

Sensitive data

Special data

Data protection roles, rights and obligations

Data Controllers

The Processor

The Data Subject

The supervisory authority (Data Protection Authority or DPA)

Cloud services

Controller Requiremnets

Summation of:

Personal Data

Transparency & Accountability

Employee rights

Data Breach Notification

How you gather data about your employees

Subject Access Requests (SARs)

Appointment of a Data Protection Officer (or “DPO”)

Record keeping

Privacy by design & Privacy Impact Assessments (PIAs)

What is lawful processing

Getting it wrong

Checklist

**The New Regulations**

To save you reading the entirety of the GPDR (*all 260 pages!)*, this guide and checklist identifies the significant changes your firm needs to understand and how to plan for those changes.

The changes should not be underestimated and this checklist will ensure you are can prepare for 25 May 2018.

The ICO says they will be making detailed plans for further GDPR guidance in the upcoming months, but say they will not be rushing to produce such guidance, and there will be no leniency regarding fines because firms have had two years to prepare!

**The right to data protection**

The EU Charter of Fundamental Rights says that everyone has the right to personal data protection in all aspects of life: at home, at work, whilst shopping, whilst receiving medical treatment, when dealing with the government or when on the Internet. This right is not only extended to EU citizens, but to all people in the world. This means that the EU not only expects governments and businesses across the world to protect the personal data of EU citizens, but also expects EU governments and businesses to protect the personal data of everyone, regardless of whether such data relates to EU citizens.

**What is personal data?**

Personal data is any and all information relating to an individual, whether it relates to their private, professional or public life. It can be anything from a name, a photo, an email address, a person’s bank details, posts on social networking websites, medical information, work performance, subscriptions, purchases, tax number, education or competencies, location, username and password, hobbies, habits, lifestyle, or a person’s computer’s IP address.

The GDPR applies when a person can be directly or indirectly identified by such data, or when a person can be uniquely singled out in a group of individuals.

**Sensitive data**

Although the GDPR does not differentiate between types of personal data based on sensitivity, some types of personal data are clearly of a more sensitive nature than others.

The GDPR highlights personal data of children as a type of personal data that requires extra care. The ‘duty of care’ argument can also be made for other categories of vulnerable people, such as the elderly. Also, data processing that poses (high) risk to the rights and freedoms of the individual is considered extra sensitive, thus requiring data protection impact assessments to be carried out prior to the processing and notifications of data breaches to supervisory authorities and individuals.

Unfortunately, the GDPR doesn’t details the personal data that would fall into the category of ‘sensitive data.’ However, based on the guidelines of supervisory authorities regarding data breach notification and classification of data in relation to data security, the following types of personal data should be regarded as having increased sensitivity:

* Special data
* Someone’s personal financial or economic data
* Data that may lead to stigmatisation of or discrimination against the individual
* Usernames, passwords, and other user credentials
* Data which are protected by a legal or professional secrecy obligation
* Data that could be misused for identity fraud.

**Special data**

There is strict prohibition to process such data, unless a specific exemption also mentioned in the GDPR applies, like a narrowly described use case (for example, employment law), a specific controller (for example, a non-profit organisation) or with the explicit consent of the individual. The data that falls into this category is:

* Data revealing racial or ethnic origin (for example, photos)
* Data revealing political opinions
* Data revealing religious or philosophical beliefs
* Data revealing trade-union membership
* Genetic data
* Biometrics
* Data concerning health
* Data concerning sex life, including sexual orientation, and
* Data related to criminal convictions, offences and related security measures

**Data protection roles, rights and obligations**

EU data protection law identifies 4 roles in data protection, each with their own obligations and rights under the GDPR, they are:

* The Data Controller
* Data Processors
* Data Subjects
* The supervisory authority (Data Protection Authority or DPA)

**Data Controllers**

The controller is the person, legal entity, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Generally, the role of the controller is derived from the organisation’s functional relation with the individual. That is, a business is the controller for the customer data it processes in relation to its clients, and an employer is the controller for the employee data they process in connection with the employment relationship. In some cases, the role of the controller is derived from the law or official tasks of the organisation.

An IFA is the controller and processes financial data in connection with making personal recommendations. The role of controller can be derived from the factual influence of an organisation over the data processing. For example, somebody who steals personal data is considered the controller for the stolen data (and lacks sufficient legal basis for the processing, making the processing illegal).

A similar argument can be made for an organisation’s headquarters, which requires its affiliates to process their data by using a specific cloud application.

As a data controller you must:

* Have a sufficient legal basis for the processing of personal data (for consent, a contract, a legal obligation or a legitimate interest which overrides the data subject’s fundamental rights, freedoms and interests)
* Hold personal data only for specified, explicit and legitimate purposes (purpose limitation)
* Limit the processing and retention of personal data to said purposes (data minimisation)
* Use the data only for secondary purposes which are compatible with the purpose for which the data were collected (use limitation)
* Ensure that the data are accurate, up-to-date and relevant (data quality)
* Take adequate measures to protect the data (security)
* Ensure that the personal data are processed in accordance with the principles of data protection by design and data protection by default;
* Inform the supervisory authorities and the data subject of a data breach
* Demonstrate compliance with the GDPR (documentation)
* Prevent personal data from being transferred to recipients in countries which do not provide an adequate level of protection compared to the GDPR (data export restrictions).

The controller is accountable for the processing of personal data and liable for any damage resulting from a violation of the GDPR rules. Where a controller processes personal data jointly with another controller, they could be jointly and severally liable towards the individual.

**The Processor**

Is a person, legal entity, public authority, agency or any other body which processes personal data on behalf of the controller (for example, a service provider). Typical processors are IT service providers (including hosting providers) and payroll administrators.

The processor is required to process the personal data in accordance with the controller’s instructions, and take adequate measures to protect the personal data. The processor may not use the personal data for its own purposes. The processor must process the personal data in accordance with the principles of data protection by design and data protection by default, inform the controller of a data breach, demonstrate compliance with the GDPR by keeping up-to-date documentation about the processing, and prevent the personal data from being transferred to recipients in countries that do not provide an adequate level of protection.

The controller is required to close a processor agreement with the processor detailing the processor’s obligations.

The processor is liable for any damage resulting from not meeting its obligations under the regulation or acting contrary to the controller’s lawful instructions. This includes liability for data breaches caused by the processor. It should be noted that the controller is liable for the damage caused by the processor, so controllers should do proper due diligence before engaging processors, supervise their processing of the personal data, and conduct regular audits and compliance checks to verify the processor’s compliance with the regulation.

**The data subject**

Is an identified individual or an individual who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other individual or legal entity.

Specific rights are extended to data subjects regarding the use of their personal data, including the right to:

* be informed about the data processing
* consent to the processing of their personal data (opt-in) or object to the processing of their personal data (opt-out)
* obtain personal data in a structured and commonly used format in order to transfer those data, in certain circumstances, to another controller (data portability)
* not to be subjected to fully automated data processing or profiling
* ask the controller whether personal data are processed about their, the right to know which data are processed (right of access)
* correct where the data are incorrect
* complete the personal data where the personal data are insufficient in relation to the purposes for which they are processed, and
* has the data erased under certain circumstances, such as where the retention period has lapsed or where consent for the processing has been withdrawn (*right to be forgotten*).

Furthermore, the data subject has the right to register a complaint with the supervisory authority and receive compensation for damages incurred as a result of noncompliance by the controller or processor.

**The supervisory authority (Data Protection Authority or DPA)**

Is the public authority that supervises and enforces the GDPR on the territory of its Member State.

Each DPA has broad enforcement powers, including the power to issues fines of €20m or 4% of global turnover, whichever is higher, in cases where the data subject’s rights have been infringed and €10m or 2% of global turnover, whichever is higher, in cases where data controllers or processors have not met the obligations of the regulation, and the power to conduct investigations and deal with complaints.

Controllers must notify the relevant DPA(s) of data breaches and certain types of processing, such as some international data transfers, require a DPA’s authorisation.

**The GDPR in relation to cloud services**

The new rules apply regardless of the means used to process the personal data. They apply to personal data stored on local servers, as well as on servers in the cloud. Cloud services pose a number of specific compliance challenges because the rules:

* Require Controllers & Processors know the location where the personal data are stored or otherwise processed.
* Severely limit the ability of entities covered by the GDPR to transfer the personal data to recipients outside the EEA, i.e. Norway, Iceland & Liechtenstein). Cloud services may use servers outside the EEA unknown to the controller or processor, or the cloud service’s data processing equipment in European territory may be remotely serviced by non-EU service providers. In all such cases the transfer of personal data must comply with the data transfer rules of the GDPR.

**Controller Requiremnets**

Data Controllers must

* take adequate security measures to protect the personal data from loss, alteration or unauthorised processing. The controller should assess whether the security measures of the processor meet the security requirements applicable to the personal data (on the basis of a risk analysis) and to the controller (on the basis of specific sectoral, contractual or organisational requirements) and must supervise the implementation of security measures by the processor by conducting regular audits. The same obligations apply to the processor using a sub-processor. However, most cloud providers do not allow their clients to provide instructions relating to data security or to conduct security audits.
* have a ‘data processing agreement’ with all processors. The agreement/contract must stipulate a number of particular obligations on the part of the processor, such as to act only on the instructions of the controller to take adequate security measures to
* protect the data from loss, alteration or unauthorised processing
* engage a sub-processor only with the prior permission of the controller
* assist the controller if necessary in response to requests for exercising data subjects’ rights
* assist the controller in meeting his obligation of notifying the supervisory authority and the data subjects of a data breach
* assist the controller in conducting a ‘data protection impact assessment’ to identify the privacy and security risks of the processing of the personal data
* hand over all personal data after the end of the processing or the termination of the service agreement. Cloud providers provide their services on the basis of terms & conditions which do not meet these requirements and which are not or are only marginally negotiable

**Summation of:**

**Personal data**

Must be collected only as necessary to the purpose, puts limits on the processing of special data (such as data revealing race, ethnic origin, biometrics, political conviction, religious or philosophical beliefs, data concerning health and sex life, union membership, and data relating to criminal convictions or offences) and puts limits on the processing of certain sensitive data, such as tax numbers and data relating to children.

This requires a detailed assessment of the functionality and data elements of applications before they are put to use. Many cloud services only unveil their full functionality and data requirements after organizations have started to use them.

The GDPR does not allow data processors to use the personal data for other purposes beyond providing the services to their customers. However, many cloud services reserve the right to use the data for all kinds of secondary purposes, such as marketing. Especially when cloud services are offered for free, cloud providers use the data in some way to generate revenues. Some cloud providers even claim full ownership of the data stored in their environment and sell the data to third parties.

The GDPR requires personal data to be erased when the purposes of use have ceased to exist. This means that organisations must specify data retention limits for the data (in advance), have the data automatically erased from their systems or organise for the data user to take an informed decision on the further retention of the data, and conduct audits to check whether the data have actually been erased. Many cloud services are not clear about their data erasure procedures or tell their users to erase data, so the organisation may be in breach of the regulation because the data are not properly erased from the cloud services.

**Transparency & Accountability**

The GDPR there is the introduction of a general requirement for organisations to be accountable about data processing and a greater emphasis on transparency. This will impact how an organisation requests data (ensuring the data subject is informed what data is being collected about them, for what purposes and how the data will be used), processes data and responds to the rights of data subjects. Organisations will need to keep up-to-date records to ensure they can demonstrate compliance with the GDPR and focus on being accountable and transparent about how they work with data.

**Employee rights**

As data subjects, employees already have a bundle of rights; the most important from the employer/HR perspective is probably the subject access right. These rights remain, however they are enhanced under the GDPR, bringing with it greater accountability and increased administration. The other rights of employees as data subjects include

(1) the right to be informed

(2) the right to be forgotten

(3) the right to data portability

(4) the right to rectification and restriction.

Such additional rights are likely to affect the current data management practices of your HR function.

**Data Breach Notification**

Under the GDPR, businesses will be required to notify data breaches within 72 hours. This new time limit means that businesses must have a clear policy for data breach notification to ensure that they are able to design their notification processes to meet the GDPR obligations. The new rules will involve your HR function.

**How you gather data about your employees**

Currently, employers have to inform all employees of the types of information they record and for what purposes. This obligation continues but in an enhanced form, and is likely to mean changes to your data protection policies, statements in contracts of employment and contracts with other workers.

**Subject Access Requests (SARs)**

The major change around SARs brought in by the GDPR is that the time limit for responding to a SAR is shortened from 40 days under the Data Protection Act 1998 to one month under GDPR. The GDPR also makes it generally easier for data subjects to make SARs, and employers, under the GDPR, will no longer be able to charge the £10 fee for dealing with SARs.

**Appointment of a Data Protection Officer (or “DPO”)**

For those firms dealing in data whose core activities involve the:

(i) Regular and systematic monitoring of data subjects on a large scale; or

(ii) Large scale processing of special categories of data (meaning the likes of health data, political opinions, religious and racial and ethnic origin data), it will be necessary to have a data protection officer.

**Record keeping**

Through the increased focus on transparency and accountability, there will be much tighter standards upon the nature of data employers can retain and for how long, meaning that the retention periods for records will need to be identified and monitored and you will also need to keep better records of your decision making process. Keeping improved records will be key to demonstrating GDPR compliance.

**Privacy by design & Privacy Impact Assessments** **PIAs**

The GDPR advocates privacy by design – which means that employers will be obliged to adopt an approach that promotes privacy and data protection compliance from the outset of any project or process. So, if you outsource your pension administration you will need to carry out Privacy Impact Assessments so that privacy is “assured” into the process.

**What is lawful processing?**

When your organisation processes personal data it should only do so where it has a lawful basis; this is a fundamental rule that underpins everything your organisation does with personal data and is key to compliance. Whilst this obligation existed under the Data Protection Act 1998, under the GDPR, the legal bases or conditions, as they are often referred, that your organisation has to meet, have, for the most part, been augmented or changed (but not necessarily all in a negative way!)

There are 6 legal bases (conditions) for processing data under the GDPR:

1. **Contractual necessity**

You need to process someone’s personal data to perform a contract you have with them; for example, providing your services

1. **Legal obligation:**

 You need to process an individual’s data because your organisation has to comply with a

 legal obligation under UK or EU law

1. **Protect life**

Necessary to protect someone’s life

1. **Official function**

You need to process data in order to carry out an official function or task which is in the public interest and you have a basis for proceeding under UK law. In most cases it will apply to public bodies.

1. **Legitimate interest**

Where you are a private-sector organisation without consent, and you have a genuine and legitimate interest (which includes commercial benefit), so long as this is not outweighed by harm to an individual’s rights (the “legitimate interest” basis).

1. **Consent**

The data subject has consented to the data processing.

Consent must be:

* freely given and unambiguous; and
* as easy to withdraw as it was to give.

In addition:

* in order to be considered to be freely given, “consent should not provide a valid ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller” (i.e. employee / employer relationships);
* the request for consent must be clearly distinguishable from the other matters in a contract / Terms of Business (ToB); and
* where the ToB / contract requires a data subject to consent to the processing of their personal data where the consent is not necessary for the performance of the service it’s likely that the consent will be invalid.

**Getting it wrong**

Fines have been significantly increased. Currently the maximum the ICO could fine is £500k but the new fines are up to the greater of:

1. 2% annual worldwide turnover for the preceding financial year of the organisations or €10 million – this is for breaches related to internal record keeping, data processor contracts, DPOs, data protection by design and default; or
2. 4% annual worldwide turnover of preceding financial year or €20 million for major breaches related to issues such as consent and data subjects’ rights.

**CHECK LIST**

#### 1 Awareness

**Change**

The GDPR will significantly amend current data protection law. Not everyone within an organisation will be aware of this.

**What you need to do**

Train staff – make them aware of the changes and the new procedures and policies necessary to comply with the GDPR.

Appoint someone to oversee compliance with the reforms

Train staff

Make changes to procedures and methods of gaining consent.

#### 2 Information you hold

**Change**

If you identify you have shared inaccurate personal data with another firm you will be required to notify the other firm of the inaccuracy.

As part of the new accountability principle, businesses will also have to be able to show how they comply with the data protection principles.

**What you need to do**

Reviewing the data you hold is going to cause lots of issues so you need a policy that allows you to verify the data you hold is accurate when you interact with your clients.

If you share clients personal data with other firms you will need a checklist/sign of process to ensure the information you share is accurate.

Review existing data protection policies and practices including employment contracts, staff handbooks and employee policies.

#### 3 Communicating Privacy Information

**Change**

Additional information must be given to individuals when their personal data is obtained. You need to give details about where their data will be held and the right to be forgotten.

**What you need to do**

Amend your disclosure documents to make sure the way you communicate data rights are clear fair and not misleading – see 4 below.

#### 4 Individuals’ rights

**Change**

Individuals will have enhanced rights to:-

* + access their information
	+ have inaccuracies corrected
	+ have information erased
	+ prevent direct marketing
	+ prevent automated decision making and profiling
	+ data portability

**What you need to do**

Amend your privacy/data protection procedures and policies to ensure that they set out each enhanced right.

Know when a Personal Impact Assessment is necessary / should be used, who should be involved and the process to be adopted.

#### 5 Subject Access Requests

**Change**

SAR request rules are changing. The 40 day timescale is now one month and no fee will be chargeable. Additional information will require to be provided to individuals e.g. about data retention periods and the right to have inaccuracies corrected.

**What you need to do**

Review and update your SAR procedure for dealing with Subject Access Requests.

#### 6 Legal basis for processing personal data

**Change**:

The legal basis for processing will need to be explained in your privacy notice and when responding to SARs.  The rights afforded to individuals will vary depending on the legal basis for data processing.

**What you need to do**

Review the data processing you do then identify and document the legal basis for processing.

#### 7 Consent

**Change**: Consent must be freely given, specific, informed, and unambiguous. The recording of consent is important as data controllers must be able to demonstrate that consent was given.

**What you need to do**

Review methods for seeking, obtaining and recording consent to ensure compliance.

####  Children

**Change**: Parental or guardian consent must be obtained to process personal information of children (i.e. those under 13 in the UK).  Consent must be verifiable and written in child friendly language.

**What you need to do**

Create and implement new practices for

1. verifying the age of individuals and
2. obtaining parental or guardian consent when processing the data of children.

#### 9 Data breaches

**Change**

The GDPR widens the number of businesses obliged to notify the ICO and private individuals of data breaches.  Failure to comply with this obligation may lead to significant fines by the ICO.

**What you need to do**

Ensure you have procedures in place to detect, investigate and report on personal data breaches. The ICO suggests assessing the types of data held and documenting which breaches trigger notification.

#### 10 Data protection by design and data protection impact assessments

**Change**

Document your privacy and data protection compliance.

**What you need to do**

Know when DPIAs should be used, who should be involved and the process to be adopted.  Look at the [ICO’s guidance on Privacy Impact Assessments](https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/)for further information.

#### 11 Oversight

Designate responsibility for the GDPR changes to someone within or outside the organisation. This will be an important role for the organisation in terms of ensuring compliance with the GDPR.