A Concise Guide to implementing GDPR in your organisation

Background to the GDPR

The General Data Protection Regulation (GDPR) comes into force on May 25th 2018, replacing the Data Protection Act 1998 (DPA).

The legislation comes from the EU. Its aim is to harmonise data protection standards across the EU and further protect the rights of the individual. It applies to all organisations based in the EU and any organization outside the EU that provides goods/services to individuals in the EU. Brexit will make no difference to its adoption in the UK. It is mirrored by similar legislation in the US and by the very large majority of nations worldwide.

The existing Data Protection Act has historically been something of a tick-box process for many companies. Under the GDPR, meaningful Data Protection will have to be given a very high priority within your corporate culture.

It affects all companies, of all sizes and serving all markets. It will affect your company, even if Data Protection hasn't really been a major issue to date.

Under this new legislation, data protection comes with an enforceable expectation that all companies are "accountable" to individuals whose data they hold. Companies will be required to keep peoples' data:

- Private,
- Up-to-date
- Collected with consent, or
- Processed lawfully.

The new regime of substantial fines makes it clear that this issue will be rigorously enforced.

And it's not just your current business processes which will be affected – in the future, all projects will need to be developed with "privacy by design" built into them from the ground up.

Maintaining your focus on profit, cost control and efficient use of time

Your company needs to maintain its focus on its profit-making business priorities, and not get side-tracked by GDPR-related bureaucracy. It's going to be essential to adopt pragmatic, effective Data Protection processes which make sure you don't fall foul of the legislation, whilst avoiding unnecessary costs in time and money.

Trading up from the DPA to the GDPR

It's not all bad news. There's a lot of misinformation in the public domain, and some rather threatening language.
If you're already properly compliant under the existing legislation then you're well on the way to being GDPR compliant. The trick is to make sure you **transfer smoothly** from the DPA to the GDPR. With advice, you can leverage off your existing DPA processes to be GDPR-compliant, and so avoid inflated costs to your company.

3 Key GDPR definitions

There are 3 important concepts / terms which underpin the GDPR:

1. **Data Subjects and their Personal Data:** Under the GDPR personal data relates to *any* data record held on a living individual, who is referred to as the Data Subject. Personal Data means information which allows a Data Subject to be identified either:
   - From the data itself (effectively by their name), or…
   - By a combination of data held in different databases which may be combined to identify the data subject, or…
   - By the potential to interrogate or manipulate the data so that someone's identity can be revealed by the context in which it's held. For example, a data record may not include someone's name, but if it includes a job title, a department and a company name, it's easy to identify who that an individual must be.

2. **Data Controller**: Think of this as the organisation who *gives the orders* on how Personal Data will be held and used. This includes:
   - How data is input and stored (digitally or on paper)
   - How it is kept up to date
   - How it is analysed, interrogated, or exploited
   - How it is manipulated or changed
   - How it is output.

   Data Controllers are the organisation which dictates what happens to the personal data they hold. They may outsource the data to a 3rd party, but they still control its use, so they remain data controllers.

   Key examples within your organisation where you will be the data controller will be:
   - HR,
   - Customer
   - Supplier databases,
   - Sales and marketing target databases;

   Its adoption will also have a significant impact on the work of:
   - Legal / compliance departments
   - Software development / IT departments

3. **Data Processor**: Think of this as the organisation who physically carries out the use / amendment / output of the data *on the instructions* of the Data Controller. They operate at arm's length from the data they store and, crucially, derive no benefit from the data itself.

   This includes::
   - An in-house department
   - A department of a multi-divisional organisation who processes data on behalf of another division
   - A 3rd party service provider
   - Databases held in the cloud

Data Processor or Data Controller?

It is very possible for an organisation to be both a Data Controller, and a Data Processor for different databases. Data Controllers may process the data in-house for their own use, or within a complex corporate structure with multiple divisions. This makes no difference – being a Processor doesn't trump being a Controller. If an organisation is the one who originally captured the data, and who makes the decisions on how that data is exploited, then they are the Data Controller.

Exploring the major changes in the GDPR
The Legal and Compliance Framework

Increased focus on Accountability and good Governance
The most significant change in the new legislation

There are 2 key legal strands to the GDPR which you must consider and plan for whenever you are processing personal data. You must be also able to demonstrate that you've done so. Those strands are:

1. The 6 Fundamental Rights of the Individual
2. Identifying when Data Processing is "lawful"

What does "Accountability" mean?
Under GDPR, Data Controllers are now legally responsible for *ensuring* that the obligations specified in both these strands are met. The new concept of "accountability" which underpins the GDPR, basically means that Data Controllers will be *measured* against the effectiveness with which they've met those obligations. Failure to do so now carries with it the risk of significant fines.

What does good "Governance" mean?
Good governance means the scheme / programme of protections a Data Controller puts in place to ensure that these legal obligations are met. Rigorous governance measures include:

- Robust, usable policies, which are…
- Thoroughly documented to demonstrate compliance…
- Translated into effective procedures which are always followed
- Deeply embedded into corporate culture, often through highly-focused training programmes

So, let's look deeper into these 2 key strands:

1. The 6 Fundamental Rights of an Individual

Data Subjects are now seen as having *fundamental rights* of *control* over their *own* Personal Data - rights which organisations *must* respect.

Whereas previously, organisations "owned" the data they held, and could exploit it as they saw fit, now Data Subjects "own" their data, and organisations can only use it with their consent. Data Controllers cannot act in a way which means that these fundamental rights are breached, and are legally accountable for making sure that this doesn't happen.

In practice, Data Controllers need to develop pragmatic, effective systems which can identify and manage the demands placed on them by these 6 Rights:

So what are these "fundamental rights", and how can you make sure you respect them?

a) Right to be informed – The External Privacy Notice
Organisations have to tell every Data Subject how their data will be processed, using language that is "concise, transparent, intelligible and easily accessible". This information must be given to the data subject at the time you obtain their data.

This right is usually addressed through your External Privacy Notice. The ICO publishes guidance on what to include in your privacy notice, and "where" you should display it (on website forms, paper etc).

b) Right of Access

Data subjects have the right to confirm that their personal data is being processed. They also have the right to have access to it. Basically this means that they have the right to see a copy of all the data a company holds on them.

This access needs to be provided free of charge (with some exceptions), and without delay (usually within one month)

To demonstrate that you are providing Right of Access, companies need to implement a process which

- Logs a data access request and timestamps it
- Verifies the identity of the data subject
- Provides the data electronically (if the request was made electronically)
- Enables the provision of data within the required timeframe.

This process should be documented and all staff trained on how to handle such a request.

c)Right of Rectification

Companies have a new obligation to make sure that data is both up-to-date and accurate. Data Subjects are entitled to have their data rectified if it is inaccurate or incomplete.

This obligation continues even after data is transferred to another Data Controller. If a company corrects data held on its own database, they must also inform any third parties who have received this data of the rectification.

In practice, companies will need to implement a process, similar to the Right of Access process, which allows a data subject to request rectification. Rectification needs to be carried out within the same required timescales as for Right of Access requests.

d) Right to erasure

An individual has the right to have their personal data deleted where there is no lawful reason for its continued processing. (For details of what “lawful” means in the context of GDPR, please see below.)

Again, as with the Right of Access, and Right of Rectification, data controllers will need to put a process in place which erases data without “undue delay”. Additionally, controllers need to take “reasonable steps” to inform third party controllers that the subject has requested erasure.

e)Right to restrict processing

There will be situations where the Data Subject has the right to restrict the processing of their Personal Data. This means the data is still held but cannot be processed in any other way. These will typically relate to situations where data accuracy is disputed by the Data Subject and is under verification.
A controller must have a process in place to restrict the processing as requested. This process must also be capable of controlling what happens once the restriction is lifted. This happens if the contested data is verified as being accurate. In this case, the Controller needs to notify the Data Subject of this, before processing is resumed and you need a system in place to make sure this happens.

f) Right to portability

This right allows individuals to *obtain* their Personal Data from a Data Controller, and *reuse* it for their own purposes, across different services. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits. Typical examples would be price comparison websites for electricity / gas etc, or for financial products (mortgages and pensions)

In practice, the Right to Portability allows Data Subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way.

Data Controllers must have systems in place which can provide that data in a commonly used format, to enable usability.

There is one further right which is not considered a fundamental right, but which you nonetheless have to provide for, is the Right to Object.

Right to object

Data subjects have the right to object to their Personal Data being processed by a Data Controller

If the subject's data is processed for marketing purposes, then the data subject may object to the processing and the data can no longer be used.

If the personal data is processed on the ground of Legitimate Interest (see p. XXX below) and the data subject believes their interests override that of the controller, then the data subject has the right to object.

The data subject may also object if their personal data is processed on the grounds of public interest unless that public interest is for scientific or historical research or statistical purposes.

Bear in mind though, an individual won't necessarily know when they do and don't have the right to object and will no doubt object regardless. Your process should allow for this.

So those are the fundamental rights. Now we'll move onto the concept of "lawful" data processing

2. When is data processing lawful?

Lawfulness, Fairness and Transparency

The GDPR states that you can only process data at all if it's *lawful* to do so.

What does this mean? How do you make sure it's lawful for your company to process data?

There are 6 bases on which you can claim that it is lawful for you to process data. The GDPR states that each of these 6 bases is equally valid, and one doesn't trump another. In all cases Data Controllers must decide which of the bases best reflects the type of processing they want to carry out, and document their decision-making process. You have to be able to demonstrate why and how you chose a particular lawful base to justify your right to process Personal Data.

a) **Consent**

Fairly obviously, it is lawful to process data if the data subject has given you their consent to do so.

However, the GDPR *significantly* tightens up the rules around consent, principally around the concept of opt-out versus opt-in consent.

Previously companies have relied on an "opt-out" approach to data collection. Companies could collect / source / buy Personal Data as they wished, needing only to provide Data Subjects with an "opt-out" after the processing had already taken place. The GDPR requires that Personal Data can only be added to a database *after* the Data Subject has have given their opt-in consent.

There are important issues which need to be addressed when obtaining consent:

- You can no longer use "pre-ticked" boxes – giving consent must involve a positive action, not a passive acceptance;
- You must be able to *prove* that the data subject gave consent

- The consent must not linked to the terms and conditions. You can't make the provision of goods or services conditional on someone giving their consent for you to hold their data;
- The data subject has the right to withdraw consent at any time;
- It must be as easy to withdraw consent as to give it;
- The language used on a request for consent must be clear and plain. (Think about writing it for a 6 year old);
- If the data subject is below the age of 16, then consent must be given by the holder of parental responsibility (proven), else the processing is not lawful.

Purpose Limitation and Consent
Even once opt-in consent has been obtained, it doesn't act as a kind of blanket consent for any and all processing. Consent has to be given with a specific purpose in mind, and its exploitation is limited to that one pre-defined use.

This can involve a fairly major change in mindset, particularly for departments such as HR or Purchasing who don't really think of themselves as being "database" departments.

Your organisation will need to learn to ask itself:

- What *kind* of data do we process,
- How many data subjects do we hold?
- Does each data subject know what we're doing with their data?
- Can we justify *why* we do things the way we do?

If the answers to these questions are unclear, it's likely that you are in danger of breaching a purpose limitation.

Beyond the issue of consent, the other 5 bases make data processing lawful, even if you don't have the consent of the data subject.

b) **Vital Interests**
A Data Controller can claim that processing data is lawful because it is in the vital interest of the Data Subject. In practice, this means processing personal data to protect someone's life. In addition, processing under "Vital Interest" must be necessary – that is, if you can reasonably protect the person's vital interests in another less intrusive way, you cannot claim that your data processing is lawful.

If you think you are likely to rely on this basis, you need to document the circumstances where it will be relevant and ensure you can justify your reasoning.

c) **Contract**
Data processing is lawful even without consent when it is necessary to fulfil a contract which the Data Subject has entered into.

An example would be the necessary processing of someone's name and address in a logistics system, in order to deliver goods or services which have been bought online. A Data Subject may have given their consent to being included on a customer database, without giving consent to being included on a delivery / logistics database. This is nonetheless lawful because, otherwise, the contract couldn't be fulfilled.

d) **Legal obligation**
Data processing is lawful when it is carried out in order to comply with a legal obligation placed on the Data Subject, or the Data Controller.

For example, employers are legally obliged to process their employees' personal data so that salary details can be passed on to HMRC. The employee can't consent, nor withhold their consent, to their data being processed in this way – the employer has a legal obligation to process it.

e) **Public Task**
This exists primarily to allow public authorities to process data without the consent of data subjects, so that they can perform a specific task in the public interest that is set out in law. An example would be processing data to issue Council Tax demands.

f) **Legitimate interests**
This is a tricky one – it's the most flexible of the "lawful" bases and many companies have relied on it as a kind of catch-all basis for "lawful" processing.

The legislation says that Legitimate Interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.

As you can see, this is a very broad definition. However, it's not always the most appropriate base for establishing whether processing is lawful:

- Legitimate Interests only exist where you use people's data in ways they would reasonably expect
- You must balance your interests against the individual's. The legitimate interests of the individual can override the legitimate interests of the Data Controller data processing would cause unjustified harm,
- There is a higher standard of protection required in terms of safeguarding the fundamental rights and interests of Data Subjects – for children in particular.
- Processing must be necessary to achieve the specific results you require from the legitimate interest – it's not a blanket permission
- Processing must have only a minimal effect on people's privacy
- You have to specify the legitimate interests you're relying on in your External Privacy Notice.

To help you gauge whether you have a Legitimate Interest basis for processing Personal Data, the ICO recommends this 3 part test:

You need to:

1. identify a legitimate interest;
2. *show* that the processing is necessary to achieve it and that the same result couldn't be achieved I in another less intrusive way.
3. *balance* it against the individual's interests, rights and freedoms.

If you do decide to use Legitimate Interest as your basis for lawful processing, you should:

- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy notice.

Transparency:
Organisations need to be able to *demonstrate* that they are compliant with the GDPR. There must be a meaningful and straightforward link between GDPR policies and their translation into any project. You not only have to have the right paperwork, but you must be able to prove that the paperwork is genuinely connected to your projects, and that the link is obvious.

Embedding GDPR within your organisation
A toolkit for smooth implementation

Making sure that your organisation is GDPR compliant can seem daunting – or at least can seem to promise lengthy exposure to time-stealing bureaucracy. In fact, this needn't be the case. Identifying and implementing a few key steps can take you to compliance relatively painlessly.

Well-structured processes, and thorough Documentation are your key allies

In order to demonstrate compliance with the GDPR, just about everything has to be documented and made ready for the ICO if requested.

Both Processors and Controllers must keep records of processing. The extent of records that need to be kept is dependent on the size of the business. If you have fewer than 250 employees then, in theory, you don't have to record as much as larger organisations. However, in reality, it is very difficult to comply with most aspects of the GDPR if you don't have a good record of everything you process. How else will you write your privacy policy, or know where your data is stored to be able to complete a subject access request if you don't have it all documented already?

The ICO publishes useful templates to help you with this documentation process, which can be found here:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

Documentation template for controllers
https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx
Documentation template for processors
https://ico.org.uk/media/for-organisations/documents/2172936/gdpr-documentation-processor-template.xlsx

You must also document:

- All your data protection policies and procedures
- Any records of consent (Controller)
- Lawful basis for processing (Controller)
- Legitimate Interest balancing test results (Controller)
- Data Privacy Impact Assessments (PIAs)

If all your key policies are carefully thought through, rigorously implemented, and internally policed by a DPO or a Data Warrior, you should not only be GDPR compliant – you can demonstrate that you are should the worst happen.

Contracts with Data Processors – what do new GDPR-compliant contracts look like?

When a Controller is using a Processor, the legislation dictates that there must be a GDPR-compliant contract in place. The ICO has provided outline guidance on what needs to be in these contracts. They should include:

- subject matter and duration of the processing;
- nature and purpose of the processing;
- types of personal data and categories of data subject;
- obligations and rights of the controller; and
- there must be terms stating:
    - the processor must only act on the written instruction of the controller;
    - the individuals working for the processor, who process the data, are subject to a duty of confidence;
    - the processor must take appropriate measures to ensure the security of processing
    - any sub processors can only be engaged with the prior consent of the data controller;
    - the processor must assist the data controller in meeting its GDPR obligations with regard to: rights of the individual, security of processing, data impact assessment, and the notification of data breaches;
    - by the choice of the controller, the processor must delete (or return) all personal data at the end of the contract;
    - the processor must submit to audits and inspections, to ensure they both meet Article 28 obligations, and let the controller know immediately if they are asked to do something infringing the GDPR.

Your Legal / Compliance department needs to ensure that new contracts are in place which meet the demands of the GDPR.

Data Protection by Design not Default
This isn't a new concept but the GDPR's emphasis on accountability makes it essential that Data Security is not a bolt-on afterthought for any new project. Data Protection needs to be prioritised as an essential design element in new projects from the very first stage of development.

And it's not just new data-reliant systems and processes which need to have Data Protection designed into them. Pre-existing systems may not have been designed with such an integrated focus on data protection. In these cases, remedial technical and organisational measures need to be retro-fitted to show that you have integrated data protection into all your processing activities.

PIAs – Privacy Impact Assessments
The GDPR enhances the requirement to carry out formal Privacy Impact Assessments (PIAs) before data is used in a way which differs from the purpose for which it was originally collected. (PIAs are also referred to as DPIAs – Data Privacy Impact Assessments). PIAs / DPIAs must be carried out under the following situations:

- When using a new technology (e.g. CRM system) and
- The processing is likely to result in a high risk to the rights and freedoms of the individual.

You not only need to put all this into place, you need to be able to prove that you have done so. You must be able to *demonstrate* that you comply with all the principles, requirements and processes contained in the legislation. And the way you do that is through documentation.

Data Protection Officer

There will be some circumstances where an organization needs to appoint a Data Protection Officer (DPO). This can be an internal or outsourced DPOaaS appointment. You need a DPO:

- if you are a public authority; or
- you do large scale regular and systematic monitoring of data subjects; or
- you process special category or criminal conviction data on large scale.

Many companies decide they wish to appoint a DPO even if they don't need one under the legislation. If you do decide to do this, they must still comply with the tasks of the DPO (see below). If you decide to appoint a DPO you must document your decision-making process and your final decision.

If you decide not to appoint a DPO then it's a good idea to appoint someone to lead your data protection efforts and be the person accountable for compliance in a similar way that the DPO would be. You cannot call this person a DPO; some companies are referring to this person as a Data Warrior because they are the identified person who will champion the cause of Data Protection within the organisation. This is often an internal appointment, without the need for the costs of a new hire.

So what does a DPO (or Data Warrior) actually do?

- Informs and advises the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitors compliance with the GDPR and other data protection laws, including managing internal data protection activities, advises on data protection impact assessments; trains staff and conducts internal audits.
- Acts as the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

Changing corporate culture – the toughest challenge?
Becoming GDPR compliant will probably require a significant change in corporate culture. It's not always easy to make such a fundamental change within the mind-set of established project teams or departments. Legal and Compliance departments may be up-to-speed on GDPR – getting the word out to other specialisms can be very challenging.

Highly specific training, focused on the differing needs of individual departments or teams, may be essential in making this change effective. Marketing staff will need training with a different focus than, for example, HR staff. Software development teams will obviously need more complex, highly-technical training which would not be suitable for other staff.

You should devise a plan to help you implement this culture change, execute it, and document both your decision-making process and the procedures you adopted.

So, now you're GDPR compliant…

You've put hard procedures in place which minimize the risk of a data breach through:

1. Respecting the 6 Fundamental Rights of the Individual
2. Ensuring that any data processing you undertake is "lawful"
3. Developing and executing effective policies and procedures to ensure GDPR compliance
4. Documenting all your decision-making processes and actions so you can demonstrate compliance

These 4 steps make up your armoury against which your Accountability and Governance regime will be tested.

Who does the testing?
Ultimately, Accountability, and also the effectiveness of Governance practices, will be policed and enforced by the Information Commissioner (ICO). However, GDPR compliance should also be policed by the Board of Directors, or other very senior company leaders, as a means of managing significant risk.

The risks to companies of non-compliance may be:

1. Reputational – the risk of causing harm to data subjects through a failure of processing compliance can be very high, depending somewhat on the nature of the business.
2. Financial - The GDPR gives the ICO new powers to impose much larger fines for non-compliance.

How much could you be fined?
Fines can be levied in 2 tiers, depending on the nature of the breach:

In deciding the level / tier of the fine, the ICO will consider these factors:

- Nature of the offence
- Gravity of the offence
- Duration of the offence
- Number of data subjects involved and the level of damage they suffered
- Previous history of compliance / non-compliance with data protection legislation

A Tier 1 fine is imposed at a lower threshold and can arise from a relatively simple failure to comply with the legislation, for example the failure to notify the ICO of a data breach within the specified timescale. It takes into account the "totality of the exposure" – simply put, how serious was the non-compliance?

Tier 1 fines can be imposed up to 2% of global turnover, or up to a maximum of £10 million.

A Tier 2 fine is imposed when there has been a breach of the fundamental rights of a Data Subject, or a fundamental failure to follow the requirements of the legislation.

Tier 2 fines can be imposed up to 4% of global turnover, up to a maximum of £20 million.

It's also important to note that a new provision under the GDPR means that Controllers can no longer push responsibility for a security breach down onto the Data Processor, as was possible under the DPA. Data Controllers have the primary responsibility for ensuring a breach doesn't occur, and are the "target" of the ICO. Data Controllers are responsible for the actions of their Data Processor.

Checklist for reducing the risk of fines through effective Breach Management
Qualified data breaches must be reported to the ICO within 72 hours of becoming aware of the breach, where feasible.

If a breach is likely to cause a high risk to an individual's rights and freedoms then you must *also* notify the Data Subject.

You must have a policy and a process in place which:

- Enables the identification of a data breach, reportable or not
- Defines what a breach is
- Assesses the severity of a breach
- Ensures that the organization knows who its regulatory authority is
- Sets out how to notify the supervisory authority within the 72 hours
- Sets out how to notify the data subjects if needed
- Sets out what information must be provided to the supervisory authority if there is a breach
- Documents a response plan for addressing any breaches
- Documents all breaches, reportable or not