Members guide to GDPR.

A Practical Introduction to the General Data Protection Regulation Written by DAMM Solutions, on behalf of the Bedfordshire Chamber of Commerce

Bedfordshire Chamber of Commerce

Members guide to GDPR.

The current legislative landscape for data protection across the European Union is fragmented, causing confusion to organisations and individuals. This will drastically change when in May 2018 a new

European privacy law is due to take effect, designed to harmonise data protection amongst it's Member States. The reform will be the toughest data protection Regulation in the world, potentially impacting any organisation that does business within the EU – Even if they hold no office there.

The existing Data Protection Act has been in place since 1998, at a time when less than 1% of Europeans had access to the internet and online privacy concerns were mostly part of science fiction. Google had yet to be launched. Since then, the internet has grown manifold, growing

the data by numbers that most people didn't even know existed (We're currently counting the zettabytes). The way this data is collected, stored, and used has also changed fundamentally, while the same outdated data protection rules have applied.

What is the GDPR?

The General Data Protection Regulation (GDPR) harmonises data protection laws in the EU that are fit for purpose in the digital age. By introducing a single law, the EU believes that it will bring better transparency to help support the rights of individuals and grow the digital economy.

The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the EU, or that collect and analyse personal data of EU residents. Even organisations outside Europe need to demonstrate compliance, or face the possibility of significant penalties.

The primary objective of the GDPR is to give citizens back control of their personal data. From an economic standpoint, the GDPR aims to simplify the regulatory environment for international business by unifying the regulation within the EU.

Because the GDPR is a Regulation and not a Directive, it means that it is directly applicable in all EU member states from 25th May 2018. The main difference is, a Directive only directs member states to implement ruling, but does not enforce.

Why does the EU want this law?

The EU states that "the Regulation is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around 2.3 billion euro a year."

One single law is instrumental to the riddance of the confusing situation where 28 separate member states all follow their own laws and regulations. Though the GDPR is very strict, once an organization is compliant it can confidently do business across the EU. The hopeful expectancy is that this will lead to a significant administrative cost- saving.

Non-compliant organisations can face fines up to 20 million euro, or 4% of annual revenue – whichever is greater. These penalties are massive and can seriously harm organizations of any size. It stresses the importance of undertaking the considerable operational reforms required to be compliant when the day arrives.

To be continued...

European legislation is inherently complicated, as 28 very different countries need to agree on the final document. It makes it all the more remarkable that regulation this strict has been agreed upon. The seriousness of the GDPR shouldn't be underestimated, which is why we will dedicate more future articles to this very important subject.

Some interesting facts.

- In 1998, when the current Data Protection Act came into force, mobile phone technology was in its infancy and Google had only recently launched. Put simply, it wasn't the digital world that we now live in.
- The (EU) General Data Protection Regulation (GDPR) replaces the Data Protection Directive – commonly known as the Data Protection Act, 1998.
- The first proposal was published on 25th January 2012 by the European Commission, with numerous amendments made over the next 36 months.
- On the 17th December 2015, the European Parliament voted to approve the final proposal document.
- On the 14th April 2016, the General Data Protection Regulation was formally adopted by the European Parliament.
- GDPR came into force across the European Union on 24th May, 2016.
- We are nearing the end of a 2year transition period for EU Member States to transpose GDPR into their national law, which is also an indication of the scale of the task for many larger organisations.
- Therefore, GDPR will be legally enforceable on 25th May 2018. There will be no "grace period".

Data Protection Directive v Data Protection Regulation.

- Currently the EU Data Protection Directive – on which our Data Protection Act, 1998 (DPA 98) is based - sets certain aims and requirements that must be achieved in each Member State. National Authorities have the flexibility to create or adapt their legislation to meet these aims. As an example, cold telemarketing to consumers is banned in Germany, while the UK allows it under certain conditions.
- The GDPR is designed to harmonise data protection laws across Europe, with a Regulation which is immediately applicable and enforceable by law in all Member States. Ie, we will be
- Adopting similar laws to those currently in place in Germany with regards to marketing.

The Myths around GDPR.

- The UK will be adopting the GDPR in full – the recent Brexit result has no bearing on our adoption of it. On 25th May 2018, we will still be EU Members, so we must comply.
- The GDPR is being interpreted into UK Law by the Data Protection Bill. This is currently passing through Parliament and will be known as the Data Protection Act 2017.
- Between now and 25th May, Parliament will repeal the current DPA 98, replacing it with GDPR, or, as we will refer to it as – the Data Protection Act, 2018.
- The only major changes the UK Government have made (at the time of writing) include the monitoring of personal data for reasons of National Security (anti-terrorism) and for Public Authorities to use Legitimate Interest as a legal basis for processing the personal data of residents in their areas.
- Compliance of the current Directive (DPA 98) or being ISO certified does not render you compliant with the GDPR. There are numerous enhancements and new guidelines with the GDPR, compared to the DPA 98 and only a very small percentage of GDPR relates to IT security.
- One of the greatest misconceptions of GDPR is from organisations who don't use data for marketing – they believe they are exempt. The GDPR covers every organisation in the EU who hold, collect, or transfer personal data within the organisation. This includes employee data. Therefore, if you have just a single employee, or a single client or supplier, then you have personal data in your business.

- We don't need to start worrying about GDPR yet – some elements have yet to be finalised. The GDPR is a published, legal document and all Articles and Recitals go into sufficient detail to be implemented into business. It is only the fine detail that we are waiting for some clarification on.
- GDPR preparation requires a change of business mindset. Businesses can no longer collect and store as much personal data as they wish to. Using a concept called Privacy by Design, you should consider the rights and freedoms of individuals over and above the commercial needs of the business.

Some Definitions.

A forward thinking attitude can help a business overcome some of today's biggest global challenges.

Personal data, or Personally Identifiable Information (PII) is defined by the Information Commissioner's Office (ICO, the Supervisory Authority for the UK) as:

"Any information relating to an identified / identifiable natural, living person"

Under the GDPR, not only does this include name, address, email address, National Insurance number, employee number, Unique Tax References and bank account details, but also location data, biometric data and online identifiers, such as IP address and Cookie data.

The GDPR refers to the personal data of every EU citizen, irrespective of where they reside in the world. If you hold EU residents' data, then you must comply.

- The Data Subject is the living individual about whom the personal data information directly concerns.
- PII – Personally Identifiable Information – any information which on its own, or when merged with other information, allows an individual to be identified.
- The Data Controller is a person who (either alone, or jointly, or in common with other persons) determines the purposes in which any personal data are, or are to be processed. **If you collect data via your website, then you are a data controller, as you are responsible for the collection of that data.**
- The Data Processor is responsible for processing personal data on behalf of a controller. **If you take receipt of data collected by the Controller and hold it or analyse it, then you become the Processor.**

- Data Breach – this is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. **Essentially, it is any instance where personal data is exposed to unauthorised persons, or when a laptop or USB stick is lost, or if an email is sent to the wrong person, or a server or website is hacked.**

- ICO – The Information Commissioner's Office. This is the UK Supervisory Authority for data protection. It is an independent body set up to uphold the rights and freedoms of individuals concerning their personal data. Every major State has a Supervisory Authority.

Preparation for GDPR.

Preparation for GDPR is a highly complex process – and this is highlighted by the two-year lead time the European Parliament have allowed. When planning your GDPR preparation, you should consider the following three key terms.

Accountability.

Document everything – the whole thought process and any decisions made. What was the logic behind each decision? Did you arrive at a decision off the back of a business decision, or was it made with the Rights and Freedoms of the data subject as your primary concern?

GDPR is a legal document and is down to interpretation of the individual circumstance. If you believe you have a worthy argument for a decision being taken, then detail this. If you can demonstrate that the rights and freedoms of the individual have been considered and are not affected, then you may have a valid point.

Transparency.

You are required to be open and transparent with the data subject. Tell them exactly what data you need from them and why. What will you be doing with it? How will you be using it and who will it be transferred to? How long will you be holding it for? You are not able to do anything that is not explained in the Privacy Policy.

Trust.

If you adhere to the Accountability and Transparency stages, then you are open with the decisions you have made, and you are communicating with the data subject(s) as to how the data is being used. This invokes Trust in your organisation.

To prepare for GDPR, the following tasks are likely to need completing:

- Readiness Assessments – this is to determine how ready (or not) specific areas of the business are. This allows you to prioritise by the areas requiring most attention. This contributes to the accountability element of GDPR as you have a record of this assessment.

- GAP Analysis – analysis of the way data is used across the business allows you to form judgements as to where respective areas of the business are regarding the DPA 98 and where you need to be for the incoming GDPR.
- Data Mapping – this is an intrinsic phase of preparation – you need to map the flow of every piece of data into, out of and across the business. The accuracy of this piece will have a direct link to your ability to react to a Subject Access Request, or a Deletion Request. This will be detailed further in the guide.
- Development of a risk-based plan – upon completion of the early stages, you will have a list of the critical areas to be addressed and the "lesser" areas ahead of 25th May. All decisions taken will require a risk-based plan which again, relates to the accountability element.

It is highly unlikely you will be 100% compliant by 25th May, due to the sheer scale of the task between now and the deadline. Instead, you should aim to achieve a **"defensible level of compliance"**. This does mean it will be an on-going process to achieve (and remain) compliant. The greatest challenge will be not to let your guard down and slip into bad habits. If you suffer a data breach, then you will need to prove you have maintained the appropriate documentation and standards of compliance – hence GDPR being a business mind-set change more than anything.

Guidance from the Information Commissioner's Office (ICO).

The ICO have taken several steps to help UK businesses prepare for GDPR. Firstly, publishing a top-level guide on how to prepare for GDPR and, secondly, launching a dedicated GDPR preparation helpline - 0303 123 1113, Option 4.

Their 12-point plan, however is an excellent place to start:

1. Information You Hold
2. Awareness / Staff Training
3. Review of Privacy Information
4. Individuals' Rights
5. Subject Access Requests
6. Lawful Basis for Processing
7. Consent
8. Children
9. Data Breach
10. Data Protection by Design
11. Data Protection Officers
12. International Data Transfers

Information You Hold.

You will need to create a data map across the business, which includes supplier, client, employee and 3rd party / marketing data and current and historical datasets. Every database needs to be meticulously analysed and critiqued:

- What personal data do you hold?
- Where did it come from – what was its source of origin?
- How was it collected / generated? If consent is the legal basis for processing, then do the permission statements satisfy the consent guidelines required under GDPR?
- How long have you had it for? What are your retention periods?
- Who do you share it with, and how? By what means?

Every time the data is transferred to a new area / department of the business and is subject to a different type of processing, you should identify your legal reason for this processing.

If you are unable to provide robust responses to any of these five questions, or identify the legal basis for processing at each stage in the data flow, then you should consider if you have a legal right to hold the data – consider deletion.

Awareness / Staff Training.

Staff will need to be made aware of GDPR and how the organisation intends to adapt to achieve compliance.

The type and nature of training required will be dictated by the size and nature of the organisation and an individual's role.

It is recommended to tailor training sessions to the specific department as each will be handling PII in a different way.

As an example, Front of House / Reception will be collecting the personal data of individuals visiting the premises, however, this information should be stored securely and out of sight of other visitors to the premises. Account Management teams will be accessing data on the CRM and sending emails to clients and suppliers. Policies will need to be written to dictate how information is transferred securely within internal departments and to external third parties.

Review of Privacy Information.

The Privacy Notice is a document that is derived from your Privacy Policy. Its purpose is to describe the personal data process, informing the data subject of their Rights and Freedoms as individuals.

Your current Privacy Notice will need to be reviewed – changes will almost certainly have to be made to reflect the shift in control and the increased rights of the data subject.

It is a legal requirement for organisations to have a Privacy Notice on their website – telling users of the site and existing customers of the organisation, however many do not comply.

Under the DPA 98, you are only obliged to summarise what you will do with personal data when it enters the business, however, the GDPR

requires you to give precise details of each process. If it is not detailed in the Privacy Notice, then you cannot do it. This relates to the transparency of processing with the data subject.

When collecting personal data, you will have to explain:

- Your justification for collecting the information you have requested – why do you need it?
- Your lawful basis for processing the data.
- Your data retention periods. You will need a data retention policy, and this will vary depending on the type of data. HMRC requires you to keep data for up to 7 years, however, few other departments have such lengthy timescales.
- How the data subject can complain to the ICO if they are not happy – explain who the ICO is and their contact details / website.
- If any third parties have access to their data and why.

This information must be presented in a clear, concise and easy to understand manner for the audience it is intended for.

Individuals' Rights.

The GDPR significantly strengthens the rights of individuals and this is detailed in Chapter 3, Articles 12-23. These aspects also reveal how even the most compliant organisations still need to prepare for GDPR.

Enhancements:

- Article 13 requires you to notify the data subject of your processing activities in detail.
- Article 16 grants the Controller the right to correct inaccurate information – currently, there is no obligation on the Controller to do this, however they will now be required to.
- Article 21 permits an individual (data subject) to object to the processing at any time, without giving a reason. The only exemption to this is if the Controller has compelling legitimate grounds to do so – for example, a Council processing for Council Tax billing, or data being processed as part of a legal investigation.

New Rights include:

- The Right of Erasure (Forgotten)
- The Right to Data Portability

Right to Erasure (Right to be Forgotten).

Under Article 17, this allows individuals to request the deletion of personal data and, where the data has been transferred across departments, or to third parties, the recipients must also comply with the request.

Data controllers must erase personal data "without undue delay" if there is no reasonable case for the data to be kept.

Referring to data mapping again, it is imperative that ALL areas of the business are checked for personal data relating to the data subject as failure to ensure absolute deletion of all appropriate records signifies a failure to comply under GDPR.

Right to Data Portability.

Article 20 details the rights individuals have to receive information about them and send it to any other organisation – even a direct competitor of the company. This has been done for some years with the "porting" of mobile numbers across networks, but this does not include the transfer of data on the individual's account.

This new right allows an individual to request the entire account to be sent to a new supplier however, the company sending the information is permitted to withhold commercially sensitive data such as spend, or discounts received.

SAR requests, the Right to Erasure and the Right to Data Portability contribute significantly to a data subject being handed back control of their own data from organisations. If all three of these rights are actioned, it can be a very laborious process, not to mention expensive from an administrative perspective.

Subject Access Requests.

This is listed under Article 15 of the GDPR and gives data subjects (including employees) the right to request a copy of any personal data an organisation holds on them – and this can be requested in a specific readable format.

This is present under the current DPA 98 and the organisation has 40 days to respond and can charge £10 "administration fee".

Under GDPR, you have only 30 days to comply, however, you are unable to charge a fee. It is likely there will be a huge increase in Subject Access Requests (SAR) and companies should formulate a process for receiving and handling these, as failure to comply with the 30-day deadline will class as a breach of GDPR.

It is essential the data mapping process is completed thoroughly as this will make handling SAR requests much easier. You will already have tracked where data flows throughout the business, so can use this mapping to plot for information retrieval.

Lawful Basis of Processing.

GDPR requires you to identify the lawful bases for your processing activity – whatever they may be. These bases should be documented, and your Privacy Notice updated to explain them.

Under Article 6 of the GDPR, the Lawful Processing must include AT LEAST one of the following:

- Consent (freely given, specific, informed, unambiguous, via clear affirmative action). It must be as easy to revoke as it is to give.
- Performance of a contract
- Compliance with legal obligation
- Protection of vital interests
- Public interests
- Legitimate interests

Consent.

At the time of writing, we are still awaiting final guidance from the ICO as to the fine detail of consent, however, Article of GDPR defines consent as:

"Any freely given, specific, informed and unambiguous indication of the subjects' wishes by which he or she, by a statement, or clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

The terms "unambiguous" and "by statement, or clear affirmative action" are new inclusions and require whoever is collecting the data to ensure there is absolute clarity on the collection of data and that the data subject is fully aware of what they are agreeing to.

- Unbundled: you must gain separate consent for opting into different channels of contact – i.e. telephone, email, SMS or postal. You also cannot force someone to sign up as a condition of receiving a service.
- Active Opt-ins. Pre-ticked boxes are invalid. Boxes must require an active tick (or similar) to ensure a clear and full indication of wishes. Statements must be clear and concise – double negative sentences must be re-written.
- You must keep complete records as to what an individual has agreed to, the method by which it was obtained and the date it was obtained.
- Companies who will be using the data, or be relying on consent should be named at the point at which consent is granted.

Article 7 states it must be as easy to withdraw consent as it is to give – and this must be explained clearly and logically before consent is obtained.

Any data capture forms, through whatever channel or medium (online or paper-based) will have to be reviewed and changes made in the way consent is sought, obtained and recorded.

If there is an existing database which relies solely on consent as its legal basis, the way in which consent is sought, obtained and recorded should be reviewed. If this does not meet the requirements of the GDPR, then you will have to gain fresh permissions from the individuals on that database to continue using it – there is a good chance that some of these individuals will not grant you this permission, in which case, the data must be deleted.

If you have sought, obtained and recorded consent in a way that satisfies the guidelines of the GDPR, then you will not have to gain fresh permissions.

You do not have to use consent as the legal basis for marketing to your existing customers. As they have an existing affiliation to you, you can use Legitimate Interest as your legal basis for processing. This is on the condition that you are only promoting similar product ranges to the individual that related to their initial purchase, however if you launch an entirely new range of products or services with no relation to those of your existing product range, then you may have to conduct a Privacy Impact Assessment to gauge the impact this would have on the data subjects. This would also be covered in your Privacy by Design review.

For B2B marketing, legitimate interest basis can again be used as it's assumed that businesses want to network and grow. This is known as the "soft opt-in", as businesses have to opt-out to stop receiving such communications.

Children.

Article 8 of the GDPR introduces specific protections for children's data by limiting their ability to consent to data processing without parent or guardian implementing a process to verify the age of individuals and / or obtaining the express permission of the parent or guardian.

This is mainly the reason that Facebook officially have a minimum age of 13 for accounts, as it reflects COPPA – the Children's Online Privacy Protection Act 1998.

The UK Government is also considering extending the Right to be Forgotten to include children's use of social media. They will be able to demand the deletion of any social media activity between the ages of 13 to 18, as their use of social media in their early teens may not reflect their more mature views when applying for jobs.

Data Breaches.

Most companies will, at some point, suffer a data breach of some description. There are so many varieties of data breach that even sending an email to the wrong person with information about an individual is classed as a breach – as is the loss of a database due to a server crashing.

You should ensure procedures are in place to detect, report and investigate a data breach. All breaches must be reported to the ICO and or the data subject within 72 hours.

There are three types of breach reporting:

1. If the breach is likely to affect the Rights and Freedoms of the data subject(s), then they must be notified directly.
2. If the breach is significant (in volume) but it does not affect the Rights and Freedoms of the subjects, then the ICO must be notified, but you do not need to contact the individuals.
3. If there is a breach, but minor (eg, a laptop is lost, but the data can be recovered via a back-up), then this must be recorded, but there is no obligation to report it.

Much of this is down to interpretation, however if in doubt, contact the ICO and ask for advice.

In terms of liability for a breach, under Article 82, the Controller is liable for any damage caused by processing which infringes the GDPR, however a Processor is only liable where they have not complied with the GDPR.

Data Protection by Design.

All documentation within the business, including Terms and Conditions, company policies contracts, the design of new products and services, and Privacy Policies, should be re-drafted with privacy as a first thought, rather than an after-thought.

When collecting data, only collect the data you absolutely NEED, rather than the data you'd LIKE. You should be able to justify the collection and use of all data. This concept is called Data Minimisation.

Data Protection Officers.

A previous draft of the GDPR suggested all companies with more than 250 employees should have a Data Protection Officer (DPO) in place.

This was changed and only the following organisations will require a DPO:

- Public Authorities
- Core activities of "regular and systematic" monitoring of data on a large scale
- Core activities of processing Special Categories of data

Your data mapping and other preparations should reveal your need for a DPO (or not).

A DPO is best recruited externally as their role is to protect the Rights and Freedoms of the data subjects – and not to answer to the commercial interests of the Board.

International Data Transfers.

If your organisation operates internationally, then you should determine which Supervisory Authority you come under.

Article 45 requires you to ensure there is an adequacy decision in place for the territory from which you are sending or receiving data – especially if it is outside of the EU.

Article 46 requires appropriate safeguards in place for these transfers – Binding Corporate Rules are an example where larger companies agree these safeguards at Board Level and in conjunction with the Supervisory Authority.

Fines.

Although the fines are an important aspect of GDPR, they should not be used as a tool to scare you into action. The likelihood of you being fined is actually very small – if you are, you probably deserve it.

Currently, the fines are capped at £500,000 for breaches and to date, the ICO has not levied the maximum fine – even Talk Talk (November 2015) were only fined £400,000, and they allowed a teenager in his bedroom

to hack their server and gain access to 150,000 customer records. Aside from the financial penalty, they lost around 1 million customers and their share price dropped 65%.

Under the GDPR, there are two levels of fines – lower level and upper level.

Lower level.

These are subject to administrative fines of up to 2% of annual (Group) turnover, or 10m euro.

- This involves a failure to obtain consent for the processing of children's data.
- Failure to maintain written records.
- Failure to report breaches when required by GDPR (within 72 hours).

Upper level.

These are subject to administrative fines of up to 4% of annual (Group) turnover, or 20m euro.

- This involves a failure adhere to the basic principles of processing (i.e. consent).
- Abuse of data subjects' rights.
- Failure to monitor and account for international data transfers.

These fines are used as a deterrent, however, if preparation for GDPR is started well in advance of 25th May 2018 and every stage of these preparations has been documented and accounted for, then you are less likely to be liable for a fine.

It's not just about the money, the ICO can take several other serious measures:

- Order a cessation of your marketing activity or halt the transfer of data within and out of your organisation for a period of its choice.
- Any action from the ICO will cause huge reputational damage. Non-compliance will suggest to the public and your customers that you may be careless with their personal data.
- Consumer-facing businesses may see an increase in subject access requests which ultimately lead to deletion requests (Right to be Forgotten).
- Aside from legal action from the ICO, there is also the potential for Civil Lawsuits – of which the ICO will provide guidance and support to the individuals. An example of this is the Morrisons employees taking class action against their employer for not safeguarding their personal data when a fellow employee stole the details of nearly 100,000 staff. This is first such data leak class action in the UK.

The Benefits of Getting It Right!

Why GDPR should be viewed as a positive step forward.

Aside from achieving compliance under GDPR, you are giving individuals a genuine choice and on-going control over how their personal data is used. It ensures you are accountable in your decisions relating to personal data and combined these to ensure trust between the company and the data subjects – whether they are employees, clients / customers, suppliers or prospective customers. The GDPR will also give you a greater understanding of the data you have in-house and ensure the quality and accuracy of it is maintained.

If a data subject trusts you in the handling of their data, then they are more likely to grant permission for it to be used throughout the business for reasons other than the basic level of processing. You may learn more about your customers and prospective customers than you were able to under the DPA 98.

Frequently Asked Questions.

Q: I've got Mailchimp - Do I need to get permission from the 20,000 end users I send promotions to? We currently have an unsubscribe option on the footer – is this sufficient?

A: This depends who the recipients are. If the recipient is B2B and they are existing customers or prospects then you may continue as long as there is an unsubscribe option at the footer. If the promotion is linked to, or is like the product line or service they received from you, then you can rely on what is termed as "legitimate interest" to continue marketing to them. If it is a B2C email broadcast and they are existing customers you can again rely on "legitimate interest".

If they are B2C PROSPECTS then this will depend on how the data has been collected and what opt-ins have been gained at the point of collection. If consent satisfies GDPR, then you can use it, if it only satisfies the Data Protection Act, then you may have to gain fresh permission from the 20,000 users.

Q: I've regularly sent unsolicited catalogues to people thinking they may wish to buy merchandise -can I still do this?

A: If it is a B2B mailing (sent to a business) then you can continue. If it is a consumer mailing (sent to an individual at their home address), then you'd be best to review how the data was collected.

Q: I collect data at an exhibition about their needs – will this change?

A: If the data collected is for B2B use, then this will not change. You can still rely on "legitimate interest" for B2B marketing. If the data collected is for consumer marketing, then you will need to gain specific opt-ins in line with the requirements of the GDPR.

Q: Do tenders now need to show and prove they are compliant with the GDPR?

A: Tender documents will start asking for evidence of your GDPR preparations to be included. This may range from a simple question relating to your preparations, to actual examples being provided. If you are not able to supply the required evidence or documentation, then this could render the decline of your tender application.

If you send out tenders to your suppliers, then it is recommended you include GDPR-relevant questions, as you will have a responsibility to ensure your supply chain complies with the Regulation.

Q: Other than a Privacy Statement, do we need to have a GDPR statement on our website?

A: No, however the Privacy Policy / Privacy Notice will need reviewing and your use of data explained specifically. If a specific use of data is not mentioned in the Privacy Notice, then you can't do it. Under the current Data Protection Act, you are only obliged to give a summary of how you intend to use the data.

Q: How do I know my GDPR statement meets the requirements? Is there a standard template?

A: There is no "standard template" in the preparation stage. The key terms to remember when preparing and implementing your GDPR plan are "Accountability" and "Transparency". If you can account for every decision you have made in your preparation and you are being transparent with the use of the data you have, then this is a very good start.

That said, DAMM Solutions are creating a set of policy templates for you to adapt to your company once you have completed your preparations.

Q: I don't have time for all this – is there someone that can help me with a data audit? ...and how much will it cost?

A: Yes. DAMM Solutions Ltd can help with this. Likewise, there are many other companies that offer similar services. Before you instruct or engage with someone, ask their experience and credentials.

The cost will typically depend upon the size and complexity of your organisation and how compliant you are with the current Data Protection Act, compared to the incoming Regulations – a Gap Analysis will need to be completed to reveal the scale of work required.

If you decide to do all preparation in-house, then you are recommended to seek professional guidance before commencing and at a later stage in the process to ensure the appropriate decisions are being taken.

Q: I've seen companies offering "simple solutions" to GDPR for a fixed fee.. is it really that easy?

A: No, it's not – and this approach, for most organisations will not offer sufficient detail. At DAMM Solutions, our team includes a marketing specialist, IT specialist and an experienced Data Privacy Lawyer from a major airline.

ICO GDPR Checklist.

How do you rank in your preparations

Step 1: Lawfulness, Fairness and Transparency

1.1 Information you hold

Your business has conducted an information audit to map data flows.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

Your business has documented what personal data you hold, where it came from, who you share it with and what you do with it.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

1.2 Lawful Bases for Processing Personal Data

Your business has identified your lawful bases for processing data and documenting the data.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

1.3 Consent

Your business has reviewed how you ask for and record consent.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

Your business has systems to record and manage ongoing consent.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

1.4 Consent to Process Children's Personal Data for Online Services

If your business relies on consent to offer online services directly to children, you have systems in place to manage it.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

1.5 Registration

Your business is currently registered with the Information Commissioner's Office.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

Step 2: Individuals' Rights

2.1 Right to be informed including privacy notices

Your business has provided privacy notices to individuals. Not yet implemented or planned

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

2.2 Communicate the Processing of Children's Personal Data

If your business offers online services directly to children, you communicate privacy information in a way that a child will understand.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

2.3 Right of Access

Your business has a process to recognise and respond to individuals' requests to access their personal data.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

2.4 Right to Rectification and Data Quality

Your business has processes to ensure that the personal data you hold remains accurate and up to date.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

2.5 Right to Erasure including Retention and Disposal

Your business has a process to securely dispose of personal data that is no longer required or where an individual has asked you to erase it.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

2.6 Right to Restrict Processing

Your business has procedures to respond to an individual's request to restrict the processing of their personal data.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

2.7 Right of Data Portability

Your business has processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

2.8 Right to Object

Your business has procedures to handle an individual's objection to the processing of their personal data.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

2.9 Rights related to Automated Decision Making Including Profiling

Your business has identified whether any of your processing operations constitute automated decision making and have procedures in place to deal with the requirements.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

Step 3: Accountability and Governance

3.1 Accountability

Your business has an appropriate data protection policy.

- [ ] Not yet implemented or planned
- [ ] Partially implemented or planned
- [ ] Successfully implemented
- [ ] Not applicable

Your business monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

- [ ] Not yet implemented or planned
- [ ] Partially implemented or planned
- [ ] Successfully implemented
- [ ] Not applicable

Your business provides data protection awareness training for all staff. Not yet implemented or planned

- [ ] Not yet implemented or planned
- [ ] Partially implemented or planned
- [ ] Successfully implemented
- [ ] Not applicable

3.2 Data Processor Contracts

Your business has a written contract with any data processors you use. Not yet implemented or planned

- [ ] Not yet implemented or planned
- [ ] Partially implemented or planned
- [ ] Successfully implemented
- [ ] Not applicable

3.3 Information Risks

Your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.

- [ ] Not yet implemented or planned
- [ ] Partially implemented or planned
- [ ] Successfully implemented
- [ ] Not applicable

3.4 Data Protection by Design

Your business has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.

- [ ] Not yet implemented or planned
- [ ] Partially implemented or planned
- [ ] Successfully implemented
- [ ] Not applicable

3.5 Data Protection Impact Assessments (DPIA)

Your business understands when you must conduct a DPIA and has processes in place to action this.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

Your business has a DPIA framework which links to your existing risk management and project management processes.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

3.6 Data Protection Officers

Your business has nominated a data protection lead or Data Protection Officer (DPO).

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

3.7 Management Responsibility

Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

Step 4: Data Security, International Transfers and Breaches

4.1 Security Policy

Your business has an information security policy supported by appropriate security measures.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

4.2 International Transfers

Your business ensures an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

4.3 Breach Notification

Your business has effective processes to identify, report, manage and resolve any personal data breaches.

- ☐ Not yet implemented or planned
- ☐ Partially implemented or planned
- ☐ Successfully implemented
- ☐ Not applicable

If the majority of your response are "not yet implemented or planned" then you are at stage one and we strongly recommend that you seek advice or guidance.

Where you have answered "Successfully implemented" or "not applicable" then we suggest that you have the necessary evidence available to demonstrate that these areas have been completed or, alternatively, why this is not applicable to your organisation.

Accountability is a key element of GDPR.

An online version of this checklist can be found on the ICO website

www.ico.org.uk

This guide has been written by DAMM Solutions Ltd. on behalf of Bedfordshire Chamber of Commerce.
DAMM Solutions are a leading, fully integrated, creative agency offering excellence in GDPR services, brand strategy, design and conventional / digital marketing solutions. Our Company Directors have in excess of over 35 years combined experience and have had the privilege of working with many of the top UK and global brands. We combine the very best strategic thinking and digital know-how with excellent creative design to provide a truly integrated marketing agency service. From our base in Bedfordshire, we design and produce Brochures, Catalogues, Websites, Social Media Platforms, Exhibitions and marketing materials for our clients throughout the UK and Worldwide. As a creative marketing agency, we have always aimed to deliver meaningful results for our customers and this has come from working closely with them to develop successful and long- standing relationships. Maybe it's time you gave us a call to discuss how our leading creative agency can benefit your business. Tel: 0372 – 683 7111 or visit our website at www.dammsolutions.co.uk

---