**Introduction**

Data is one of our greatest assets. We benefit from the personal data we hold achieving competitive advantage to deliver high quality insight and analysis, information, news and entertainment to our customers. In order to use the personal data we hold we need to comply with certain minimum standards. The minimum standards required by the Group are based on the EU General Data Protection Regulation (GDPR).

This means that the data we hold should be:

1. Collected for specific and lawful purpose
2. Not collected unnecessarily
3. Accurate and kept up to date
4. Only stored for the necessary period
5. Protected using adequate safeguards

Good data handling will drive tangible commercial benefits for your business as well as being the right thing to do.
Benefits of good data handling

• Increases customer confidence and builds trust in your brand, leading to an increasing willingness to use your business. Good data handling drives a competitive advantage.

• Minimises complaints and disputes with your customers which fosters good corporate reputation.

• Ensuring that your business follows good data handling will reduce the risk of falling foul of data protection law.

• Adherence to good data handling practices will inevitably lead to data minimisation i.e. only collecting relevant data and using it for the original purpose for which it was collected, which will again mitigate the risk of non-compliance.

• Even if the worst case happens and a breach occurs, a more limited amount of data is compromised which reduces risk exposure.

• Data minimisation also results in cost savings as holding only the data you need should lead to a reduction in hosting, archiving and storage costs.
How do I apply the five principles?

1. Collected for specific and lawful purpose: This means the data collection is either to fulfil a contract, and/or the data subject has provided their explicit consent to the processing. You should not collect personal data and use it to market unrelated products or services without consent.

   Customers must also be offered the opportunity to opt out of any further communication.

2. Not collected unnecessarily: What is meant by “necessary”? What is commercially desirable does not always equate with what is legally permitted. Only collect data which you specifically need to provide your customer with the relevant product, service or marketing activity offered, if you don’t need it don’t collect it. This is called data minimisation.

3. Accurate and kept up to date: You need to ensure that the data you store is and remains accurate. For example; if the addresses you hold are out of date, a customer no longer works for the same company you have listed in your records, or their marketing preferences are incorrectly captured.

   It is difficult to verify the accuracy of all data provided by your customers, but you can reduce the risk of holding incorrect data by:

   • making sure you have accurately documented information provided by the customer, and
   • taking reasonable steps to ensure the accuracy of the information e.g. by confirming this with the customer.

How can you check, for example, the address you have for a customer is correct without being a nuisance? The best time to raise this with your customer is during the normal course of business, such as when renewing a subscription to a product or when a customer expands their use of your services.

Helpful tools at the data capture stage include requiring email addresses to be entered twice and having a postcode look up function.

You must also ensure that marketing preferences and consent records are accurate. Under GDPR you are required to have evidence of individual consent and connect the specific wording used
at the time that consent was provided. (This is particularly important where data use and consent notices change over time.)

4. **Only stored for the necessary period:**
   Personal data should not be stored (in a form which permits identification of the data subject) for longer than is necessary, for the purpose which it is collected. Again, what is meant by “necessary”? There is no hard and fast rule governing the length of retention periods – this depends on your business, the services provided and the type of data. So it’s a case by case review across your products and services. For more information see the DMGT Guide on Data Retention.

5. **Protected using adequate safeguards:**
   Personal data should be protected against accidental or unlawful destruction, loss, alteration and disclosure. This means that data should be protected from internal and external threats and also be safely disposed or destroyed when no longer required.

   In practice this will require implementing controls and processes detailed in the DMGT Information Security Standards.
Anonymisation

This is the process of removing personally identifiable information from data.

Extracting the value of personal data does not always need to involve retaining names and addresses etc. Fewer legal restrictions apply to anonymised data as, when done effectively, there is a low risk of disclosure of personal data.

Examples of uses of anonymised data include statistical analysis, modelling and disclosure to the public for transparency reasons.

In reality it can be difficult to determine if data has been successfully anonymised or is still personal data. Simply removing a single identifier (e.g. name or staff ID number) will not render the full data record anonymous.

Methods of anonymising data:

- aggregating data; (e.g. using age ranges rather than the specific age)
- redacting addresses and contact details from documents and using false place names and imprecise dates
- “hashing” financial details
- “de-personalising” information; Removing names or replacing with false names although unlikely to result in full, technical anonymisation of the data record.

Re-identification

When deciding how to anonymise data, be aware of the risk of re-identification. This is the real risk with anonymising data. Whilst disclosing anonymised data does not itself involve disclosure of personal data, there is a risk that recipients of anonymised data will have access to other data sets which will allow re-identification. Sometimes the limited dataset could apply to only certain individuals e.g. details of an “anonymised” employee are released with a job title that is unique to a specific individual. In general, the more precise or complete the information, the more possible it becomes to re-identify. It is important to carry out a risk assessment, which should be repeated regularly to address technological advances that may threaten the safety of anonymised data.

Governance structure: if your business seeks to truly anonymise data, there should be an effective governance structure in place to oversee the procedure, authorise the anonymisation as well as deal with consequences in the event of re-identification. Privacy impact assessments and staff training should also be part of this.
Other things to consider

Clear internal procedures: Ensuring that customers continue to trust us with their data is critical. It is all of our responsibility to ensure that we all are informed about good data handling and know what the right procedures are. Policies should be clear and conveyed to everyone who will need to deal with customer data. Using the information in this Guide as the basis for your policy, or checking that your policy is still right for your business, is a good starting point. Cascade the online good data handling training amongst your team.

Constant evaluation of procedures: Once you have policies in place to promote good data handling practices across your businesses, these need to be regularly evaluated so that they are efficient and produce the desired results for your business and meet your needs, as well as those of your customers and employees.

Adopt a privacy by design and default approach: This means that you build in maximum privacy considerations at the start. Privacy impact assessments may be required before changing or implementing data intensive products or services. They help you check to see what level of data protection already exists and what additional protections are necessary potentially avoiding issues and additional costs arising later in the process.

Turn the page to see a case study on how data handling works in practice.
Case Study

Data handling – how it works in practice
In August 2016, ABC Events start collecting data from individuals, including Mr Frost, who wishes to attend the International Building and Construction Show (IBC Show) in November 2016.

The information collected include Mr Frost's name, work email address, details of the company he works for, his telephone number, date of birth and personal address. When collecting this information, Mr Frost consents to be contacted for future IBC Shows.

Mr Frost attends the IBC November 2016 Show, which was a big success and Mr Frost is happy that he will be contacted for 2017's event.

1. In January 2017 a team member from ABC Events uses the IBC Show registration list to market for the Global Petroleum Online Directory 2017. Mr Frost is contacted about this product, which is completely unrelated to his field of work, and is annoyed about the unnecessary admin created to unsubscribe to these emails.

In July, Mr Frost accepts a job offer in a competing company and contacts ABC Events to inform them about his change of job and contact details.

2. ABC Events start circulating brochures about the IBC Show 2017 in August 2017, but unfortunately Mr Frost does not receive them as his new address was incorrectly recorded. However post is still being delivered to his old work address and Mr Frost gets a call from his old employer complaining about this. Mr Frost does not attend another ABC Events conference.

3. In January 2020, an ABC Events employee is asked by an outsourced mailing company to provide a customer list. The employee, assuming no harm will be done, provides the registration database for each ABC event held, including the 2017 IBC Show Registration list.

4. Upon receiving new marketing documents from ABC Events, Mr Frost contacts ABC Events to request that his details are removed from their mailing lists and he makes a data subject access request (SAR) to obtain a copy of all the records held about him. ABC Events do not have a system to keep track of an individual's record so is unable to locate all the information and respond to the request within the one month deadline. This is a breach of the Data Protection Regulation.
Case Study
What went wrong?

1. **Improper use** - the IBC registration list was used for a different product, which is unrelated to Mr Frost’s field and not part of the consent obtained. This may have been avoided if the team member was adequately informed of how to use customer data.

2. **Inaccurate information** - this illustrates the importance of taking steps to ensure that customer data is captured accurately. As a consequence of not recording Mr Frost’s change to email address correctly, Mr Frost missed the opportunity to be contacted about the upcoming event meaning, ABC Events has potentially missed a sale, and the error has also caused Mr Frost inconvenience by having to deal with the complaint from his old employer. This error erodes trust between Mr Frost and ABC Events.

3. **Data breach** - Loss or Unauthorised disclosure of data is the biggest risk your company will face. In this example, this could have been prevented if the data was not retained for such a long period after Mr Frost had not attended an event.

4. **Non-compliance with data protection laws** - As a result of poor data handling procedures and inefficient systems, ABC Events is not able to comply with the SAR and can be exposed to being investigated by the relevant data protection authority with a risk of possible enforcement action against ABC Events including costly fines.

5. **Access to personal data** - Proper safeguards include ensuring that only those who need access to customer and personal data are permitted. If such safeguards were in place, the old database would not have been accessible.

6. **Unnecessary collection** - note that the information originally collected included Mr Frost’s date of birth and personal address. There did not seem to be a reason why this information was collected and as a result of this leak, more of Mr Frost’s personal information has been exposed. This could have been avoided if the principle of data minimisation was followed.

Apply the lessons learnt to your own data handling practices and avoid the problem that can arise from poor data handling.
Frequently Asked Questions

1. What are my specific obligations when dealing with personal data?
   You must follow the five principles of data protection in the EU GDPR:
   - Collected for specific and lawful purpose
   - Not collected unnecessarily
   - Accurate & kept up to date
   - Only stored for the necessary period
   - Protected using adequate safeguards

   These principles should be at the heart of your practices, which should be regularly evaluated to ensure that your business is compliant where necessary.

2. What recourse do my customers have if I handle their data incorrectly?
   A formal complaint can be made to the UK data protection authority, which could result in an investigation or costly fine. Your customers also have a right to apply to court for an order requesting you to rectify, block, erase or destroy the inaccurate information. Realistically, you should invite your customers to contact you in the first instance if they become aware that information you hold is inaccurate. By maintaining an open dialogue between you and your customer, you will minimise the risk of complaints and disputes and more importantly increases customer confidence in your organisation. Similar protections apply in other jurisdictions.

3. Do I need consent to produce or disclose anonymised data?
   Not necessarily. Consent is only needed if there is a likelihood of harm being caused to the individual. However in most cases, if anonymisation is done effectively, there will be no such risk and therefore no need for consent. In considering whether or not to obtain consent for anonymising data, consider whether this is practical i.e. how many people are concerned and are they easily contactable? If, at the point of originally collecting their data, they provided consent for research purposes, then using anonymised data for such purposes is captured here. Be careful where consent was only obtained for a very narrow or specific purpose.

4. I’ve removed the names from our customer data - is this enough?
   No. Remember personal data covers more than just names and addresses. It extends to any data that can be used to personally identify an individual when combined with other information that is publicly available. Consider what other information is in your (or the intended recipient’s) control and whether this can be combined to identify an individual. If so, consider using other methods of anonymising data other than redaction.
5. **Can I wait for my customers to update their details?**
A reactive approach is more risky for your business as ultimately you are responsible for the accuracy of the personal data you hold. However, privacy laws recognise this is impractical and you are unlikely to be held to be in breach of data protection laws providing the data was recorded accurately in the first place and you have taken reasonable steps to ensure the accuracy of the information. A safer, more proactive approach may be better where you ask your customers to verify the accuracy of the information you hold. This can be done by an automated email, perhaps every 12 months, inviting your customers to notify you of any change in their details and to confirm the current information you hold. This has the added commercial benefit of staying in contact with your customers.

6. **We outsource some data processing to a third party, what do I need to consider?**
As controller of the data it is your responsibility to ensure that the third party is also meeting the requirements of the GDPR with organisational and technical safeguards.

In practice this means mandating data protection obligations through formal contracts and obtaining assurances that these obligations have been met. Although under GDPR greater liability is placed on third party processors – the ultimate responsibility for the security of your customers, contacts and employees personal data sits with your business.

7. **I’ve made sure I know our internal policies. Is there anything else I need to do?**
Yes. Make sure everyone handling customer data also know your internal policies. It is easy to forget that data breaches are not just caused by technology - most breaches are caused by human error. It just takes one mistake, but can be prevented by ensuring the staff in your business are clearly informed of the policies in place. Your business will grow and adapt to your customers needs, so you should ensure that your staff have refreshers on your policies to ensure that everyone in your business is up to date. Cascade this guide and the online Good Data Handling training to your teams.

8. **Will my business incur additional cost by doing all of this?**
No. This is another major benefit for your business, as good data handling and compliance with data protection obligations will ultimately result in cost savings for your company and reduce the like hood of costly fines for non-compliance.
## Contact

<table>
<thead>
<tr>
<th>Vicky Benham-Burr</th>
<th>Catherine Lye</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Manager</td>
<td>Senior Risk Manager</td>
</tr>
<tr>
<td>Email: <a href="mailto:Vicky.Benham-Burr@dmgt.com">Vicky.Benham-Burr@dmgt.com</a></td>
<td>Email: <a href="mailto:Catherine.Lye@dmgt.com">Catherine.Lye@dmgt.com</a></td>
</tr>
<tr>
<td>Office: +44 (0)20 3615 2937</td>
<td>Office: +44 (0)20 3615 2938</td>
</tr>
<tr>
<td>Mobile: +44 (0)7795 451028</td>
<td>Mobile: +44 (0)7867 907539</td>
</tr>
</tbody>
</table>