GDPR

THE ROAD TO COMPLIANCE – A GUIDE

DLM GROUP
MANAGING YOUR WORKFLOW

The DLM road to GDPR Compliance

12 **International**
If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you will have to determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

11 **Data Protection Officers**
You will have to consider whether you are required to formally designate a Data Protection Officer. If so, DLM will designate someone to take responsibility for data protection compliance and assess where this role will sit within your structure and governance.

10 **Data Protection by Design and Data Protection Impact Assessments**
You need to have these carried out in order to understand where you are today and when any process is added or amended. You will then work out how and when to implement them. Speak to us about how we can help

9 **Children**
It is vitally important that you start thinking about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data activity.

8 **Data breaches**
DLM will make sure you have the right procedures in place to detect, report and investigate any personal data breaches.

7 **Consent**
Consent must be given and it is very important that you refresh existing consents to meet the GDPR standard. Review how you record and manage consent and whether you need to make changes.

6 **Lawful basis for processing personal data**
Identify the lawful basis for your processing activity in the GDPR, and make sure you document it and update your privacy notice to explain it.

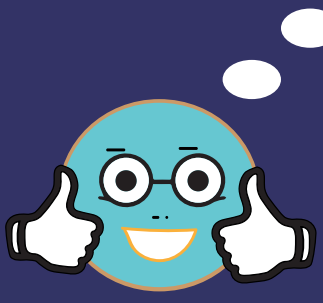
5 **Subject access requests**
DLM will help you update your procedures and plan how you will handle requests within the new schedules.

4 **Individuals' rights**
Check procedures to ensure they cover all individuals' rights. Also, will you be able to segment the data in order to show what needs to be held under other lawful reasons?

3 **Communicating private information**
DLM will help you review your current privacy notices and we will enable a plan for making the necessary changes in time for GDPR compliance.

2 **Information that you possess**
You may need to organise an information audit – documenting such details as what personal data you have, where it was accessed from and who you have share it with.

1 **Awareness**
DLM will make sure that decision makers and key people in your organisation are aware that the law is changing. This is likely to have a huge impact on businesses.



DLM GROUP
MANAGING YOUR WORKFLOW

THIS CHECKLIST HIGHLIGHTS the 12 steps you can take now to prepare for the General Data Protection Regulation (GDPR) which will come into force from 25 May 2018.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

It is important to use this checklist and other Information Commissioner's Office (ICO) resources to work out the main differences between the current law and the GDPR. The ICO is producing new guidance and other tools to assist you, as well as contributing to guidance that the Article 29 Working Party is producing at the European level. These are all available via the DLM's Overview of the General Data Protection Regulation.

It is essential to plan your approach to GDPR compliance now and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions.

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

1. Awareness

May 25, 2018 is the day the most important changes to data protection laws will be activated, so now is the time to prepare for the General Data Protection Regulation (GDPR). Awareness isn't just about reading latest updates, it has to be thorough and applied. Awareness is also about sharing knowledge and making sure that staff and members of any business or organisation are fully cognisant of what these new rules actually mean for institutions and individuals. I will make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. This is likely to have a huge impact on businesses and organisations – the figures could be truly astonishing (and in some cases, deeply worrying). EU regulators have the right to impose huge fines for violations.

Key points to consider

- How will your business or employer provide training?
- Will there be an induction programme for new staff?
- How will the new process be implemented?
- Will there be a how-to guide in case of an information request and where will it be stored?

How DLM Group can help

- Workshops
- Training program with exam quiz
- Induction hand book
- Technology to hosted Internal documents
- Technology to enhance your processes.

2. Information that you possess

You may need to organise an information audit – documenting what personal data you have on employees or members, where it came from and who you share it with. You will be held responsible for any inaccuracies in data passed on to another party so it is essential that information is checked, updated and recorded. Transparency is essential here which is why regular audits will reflect efficiency and protect you and your organisation.

Key points to consider

- Do you know what information you process?
- Why do you process it?
- Is certain information required under other regulation and if challenged can be justified?
- Does the business, supplier, or even employer have consent to process the information?
- Is there information being processed for anyone under the age of 16? Is there clear consent given by the parent or guardian?

3. Communicating private information

I will help you review your current privacy notices and we will enable a plan for making the necessary changes in time for GDPR compliance. The rationale of accessing and sharing information could be put under the spotlight so it is important that an organisation's Data Protection Officer communicates what people can or cannot do within an organisation.

Key points to consider

- Are your notices easy to read?
- Are your notices easy to access such as via the website
- What data are you collecting and for what purpose?
- Are you up to date with the Privacy notice code of practise.

4. Individuals' rights

Check procedures to ensure they cover all individuals' rights, including how you would delete personal data when necessary or the provision of data in a commonly used format electronically. Particularly important are the rights of minors or vulnerable people but also being minded of while we live in a world of ever-expanding social media, people still have the right to privacy.

The GDPR includes the following rights for individuals:
The right to be informed, of access, to rectification, to erasure, to restrict processing, to data portability, the right to object and the right not to be subject to automated decision-making including profiling.

Key points to consider

- Can you separate the data into what needs to be kept for other legal reason?
- Have you published the procedure on how to exercise the individual's rights?
- Have you carried out training on the new rights and made your business aware?
- Have you appointed a DPO yet incorporate this into your procedures?

5. Subject access requests

DLM will help you update your procedures and plan how you will handle requests within the new schedules. Again rationale is important here as is awareness of sensitive subjects like ex-employees, possible claims and litigation. The time to respond to an access request has been reduced from 40 days to 30 so it is very important that you have response plans in place.

Key points to consider

- Do you currently charge for access request?
- Will you be able to comply within one month of the request?
- How do you handle such request now and how will you going forwards?

6. Lawful basis for processing personal data

Identify the lawful basis for your processing activity in the GDPR, and make sure you document it and update your privacy notice to explain it. Up until now this has few practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your basis for processing their personal data. Basically, people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

Key points to consider

- What data do you collect and store?
- What lawful reason do you collect said data?
- Have you published the lawful basis why you collect data with in your privacy statement?
- What is your data deletion policy?

7. Consent

It is very important that you refresh existing consents if they don't meet the GDPR standard. Review how you record and manage consent and whether you need to make any changes. The key elements of the consent definition remain – it must be freely given, specific, informed, and there must be an indication signifying agreement. However, the GDPR is clearer that the indication must be unambiguous and there are new provisions, and a greater emphasis will be on individuals having clear choices upfront and ongoing control over their consent.

Key points to consider

- Do you have to gain consent for your current data?
- How can you prove you gained consent?
- How do you request opt ins and outs? Is this just a tick box?
- Do you have statements such as by using our website or you accept our terms and conditions?

8. Data breaches

You must have the right procedures in place to detect, report and investigate any personal data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Key points to consider

- Do you have remote workers with unauthorised users accessing data?
- Do you have third party business visit/ work on your premises who can access your data?
- What is your procedures to detect breaches?
- How will you notify everyone upon a breach?
- Will you need to appoint a PR representation?
- Do you have the relevant insurances such as cyber insurances?

9. Children

It is vitally important that you start thinking about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data activity. The rights of children and vulnerable people will be taken very seriously under the new rulings and has to be addressed with great sensitivity and responsibility.

Key points to consider

- Can you provide evidence that a person holding parental responsibility has given consent?
- Do you offer online services that will need consent given?
- Do you have a privacy notice written for a child?

10. Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself with the ICO's code of practice on Privacy Impact Assessments (PIAs) as well as the latest guidance from the Article 29 Working Party. You will then work out how and when to implement them in your organisation. The GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as Data Protection Impact Assessments or DPIAs – mandatory in certain circumstances.

Key points to consider

- Do you have a privacy by design best practice?
- Have you started carrying out your PIA? Has this be done by an expert?
- Do you carry out profiling?
- Do you have a framework to use any time you change a process or supplier etc?

11. Data Protection Officers

You will have to consider whether you are required to formally designate a Data Protection Officer. If so, I will designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You must designate a DPO if you are a public authority, an organisation that carries out the regular and systematic monitoring of individuals on a large scale, an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

Key points to consider

- Are you going to employee a DPO or outsource?
- Do you need one?
- Are you a health provider, education establishment, public body, Insurance/finance or legal organisation? If so then it is strongly advised you appoint a DPO
- Are you considered to carry out large amounts of processing?
- Are you familiar with the Article 29 Working Party clarifications around a DPO?

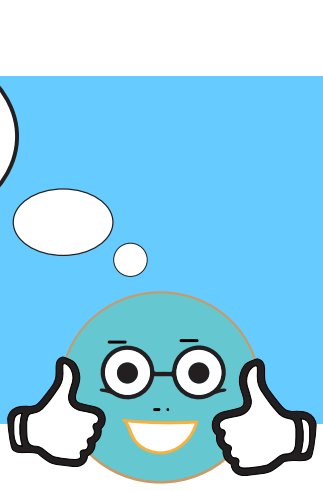
12. International

The GDPR is designed to unify data privacy requirements across all 28 EU member states. End users, customers and employees have the right to make a claim if their data is not protected in compliance with the GDPR regulations. If your organisation operates in more than one of the member states (i.e. you carry out cross-border processing), you will have to determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Key points to consider

- What software do you or your suppliers use that is based outside the UK
- Do you operate across borders?
- Do you have clients in different countries?

For further information, go to DLM-group.co.uk where you can access white papers, advice and guidance.
To find out more, or for a one-to-one free meeting please call us on: 01903 255389 or email info@dlm-group.co.uk



DLM GROUP
MANAGING YOUR WORKFLOW