CHECKLIST | 12 STEPS TO PREPARE FOR THE GDPR

Presented by Robison & Co Ltd

On 25 May 2018, the General Data Protection Regulation (GDPR) comes into effect in the EU and across the United Kingdom. The GDPR replaces the Data Protection Act (DPA) and ushers in expanded rights to individuals and their data, and places greater obligations on businesses and other entities that process personal data.

Many of the GDPR's main concepts and principles are the same as those in the DPA, so if you are complying properly with the DPA much of your approach to compliance will remain valid under the GDPR and can be a 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 essential to plan your approach to GDPR compliance now and to gain buy-in from key people in your organisation. That is why Robison & Co Ltd is here with guidance and a checklist from the Information Commissioner's Office (ICO) to help you prepare for compliance in 2018.

Compliance with all the areas listed in this checklist will require you to review your approach to governance and how you manage data protection. Use the following checklist to map out which parts of the GDPR will have the greatest impact on your business model, and create a plan to focus on those areas in your planning process.

STEP 1: AWARENESS Make sure that decision makers and key people in your organisation are aware that the law is changing. They need to appreciate the GDPR's impact.	YES	NO	ADDITIONAL NOTES
Are the key decision makers at your organisation aware that the GDPR will force you to change the way you conduct business?	☐	☐	
Do the key decision makers know how the GDPR will affect your organisation?	☐	☐	
Do the key decision makers at your organisation know what the requirements of the GDPR are?	☐	☐	
Do the key decision makers at your organisation have a plan for how you will become GDPR compliant?	☐	☐	

STEP 2: INFORMATION YOU HOLD Document what personal data you hold, where it came from and with whom you share it. You may need to organise an internal audit.	YES	NO	ADDITIONAL NOTES
Has your organisation documented what personal data you hold?	☐	☐	
Has your organisation documented where the personal data came from?	☐	☐	
Has your organisation documented with whom you share personal data?	☐	☐	
Has your organisation conducted an information audit on the personal data you hold?	☐	☐	

STEP 3: COMMUNICATING PRIVACY INFORMATION Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.	YES	NO	ADDITIONAL NOTES
Has your organisation reviewed its current privacy notices?	☐	☐	
Does your organisation have a plan in place for making necessary changes to your privacy notices?	☐	☐	
Does your organisation know what changes need to be made in order to comply with the GDPR?	☐	☐	

STEP 4: INDIVIDUALS' RIGHTS Check your procedures to ensure they cover individuals' rights, including how you would delete personal data or provide data electronically in a commonly used format.	YES	NO	ADDITIONAL NOTES
Do your procedures cover all the rights that individuals have under the GDPR?	☐	☐	
Do your procedures allow individuals to delete their personal data?	☐	☐	
When deleting personal data, would your systems help you locate and delete data?	☐	☐	
Who will make the decisions about deletion?	☐	☐	
Do your procedures provide individuals with their data electronically and in a commonly used format?	☐	☐	

STEP 5: SUBJECT ACCESS REQUESTS Update your procedures and plan how you will handle requests within the new timescales and provide any additional information.	YES	NO	ADDITIONAL NOTES
Has your organisation updated its procedures for how you will handle subject access requests?	☐	☐	
Will your organisation be able to comply with subject access requests within one month, rather than the DPA's 40 days?	☐	☐	
Does your organisation have a plan for how it will handle subject access requests?	☐	☐	
Is your organisation ready to refuse a request, which will involve you telling the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy? Will you be able to do this without undue delay, and within one month?	☐	☐	
Is your organisation able to provide additional information upon request about subject access?	☐	☐	

STEP 6: LAWFUL BASIS FOR PROCESSING PERSONAL DATA Identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.	YES	NO	ADDITIONAL NOTES
Has your organisation identified the lawful basis for your processing in the GDPR?	☐	☐	
Does your organisation have a method to document how you process personal data?	☐	☐	
Has your organisation updated your privacy notice to reflect the lawful basis for processing personal data?	☐	☐	

STEP 7: CONSENT Review how you seek, record and manage consent, and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.	YES	NO	ADDITIONAL NOTES
Has your organisation reviewed how it seeks consent?	☐	☐	
Has your organisation reviewed how it records consent?	☐	☐	
Has your organisation reviewed how it manages consent?	☐	☐	
Does your organisation need to make any changes in its process of obtaining consent?	☐	☐	
Does your organisation have simple ways for people to withdraw consent?	☐	☐	
Is your consent separate from other terms and conditions?	☐	☐	
Can your organisation's existing consents be updated to meet the GDPR standard, meaning are they specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn?	☐	☐	

STEP 8: CHILDREN Think about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.	YES	NO	ADDITIONAL NOTES
Does your organisation have a system in place to verify individuals' ages?	☐	☐	
Does your organisation have a system in place to obtain parental or guardian consent for any data processing activity?	☐	☐	

STEP 9: DATA BREACHES Make sure you have the right procedures in place to detect, report and investigate a personal data breach.	YES	NO	ADDITIONAL NOTES
Does your organisation have a procedure in place to detect a personal data breach?	☐	☐	
Now that the GDPR introduces a duty on all organisations to report certain types of data breaches to the ICO, and, in some cases, to individuals, does your organisation have a procedure in place to report a personal data breach?	☐	☐	
Does your organisation have a procedure in place to investigate a personal data breach?	☐	☐	
Does your organisation need to assess the type of personal data it holds and document when it would be required to notify the ICO or affected individuals if a breach occurred?	☐	☐	

STEP 10: DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS Familiarise yourself with the ICO's code of practice on privacy impact assessments as well as the latest guidance from the Article 29 Working Party, and figure out how and when to implement them in your organisation.	YES	NO	ADDITIONAL NOTES
Is your organisation familiar with the ICO's code of practice on privacy impact assessments?	☐	☐	
Does your organisation have a strategy on how and when to implement the ICO's code of practice on privacy impact assessments?	☐	☐	
Is your organisation familiar with the latest guidance from Article 29 Working Party?	☐	☐	
Does your organisation know how and when to implement Article 29 Working Party?	☐	☐	
Does your organisation know whether it is required to undertake a data protection impact assessment (DPIA)? DPIAs are required in situations where data processing is likely to result in high risk to individuals, such as when a new technology is deployed or when a profiling operation is likely to significantly affect individuals.	☐	☐	

STEP 11: DATA PROTECTION OFFICERS Designate someone to take responsibility for data protection compliance and assess where this role will sit in your organisation's structure and governance arrangements. Consider whether you are required to formally designate a data protection officer.	YES	NO	ADDITIONAL NOTES
Has your organisation designated someone to take responsibility for data protection compliance?	☐	☐	
Has your organisation considered whether it is required to formally designate a data protection officer (DPO)? You must designate a DPO if you are a public authority, an organisation that carries out regular and systematic monitoring of individuals on a large scale, or an organisation that carries out the large scale processing of special categories of data, such as health records or information about criminal convictions.	☐	☐	
Has your organisation assessed where the data protection officer(s) will sit within your organisation's structure and governance arrangements?	☐	☐	

STEP 12: INTERNATIONAL If your firm operates in more than one EU member state, including carrying out cross-border processing, you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you.	YES	NO	ADDITIONAL NOTES
Does your organisation operate in more than one EU member state?	☐	☐	
If your organisation has establishments in more than one EU member state or you have a single establishment that carries out processing that substantially affects individuals in other EU states, has your organisation mapped out where it makes its most significant decisions about its processing activities? This will help to determine your 'main establishment' and, therefore, your lead supervisory authority.	☐	☐	
Has your organisation determined your lead data protection supervisory authority? Use Article 29 Working Party guidelines to determine this.	☐	☐	