 8 November 2017

|  |  |  |
| --- | --- | --- |
|  | | |
| **10 Steps to prepare for the GDPR** | | |
|  | | |
|  |  |  |
| In our last edition of the IABM Journal, Rebecca Collard of Harbottle & Lewis LLC gave us an outline of the forthcoming General Data Protection Regulation (GDPR). In this edition, Nicola Bardon, Associate at Harbottle & Lewis gives us further advice on practical steps companies need to take in order to be ready for when the GDPR comes into force on 25th May 2018.  The digital world has changed dramatically over the last 20 years and so too has how we provide, collect and use personal data. The GDPR is set to drastically change data protection laws across the EU from next May. While the basic data protection principles remain under the GDPR, they have been reconstructed and the requirements to satisfy them made stronger, with much harsher fines for failing to comply. But there is no need to panic! There’s still 6 months to prepare for the new legislation. Below, we have covered the key steps that you should be taking now to help you to prepare your organisation to comply with the new framework.   1. **Awareness, training and accountability**   The overarching principle of accountability, set out at Article 5(2), applies to all aspects of the GDPR. This means that the data controller is responsible for compliance with the principles relating to the processing of personal data and the rest of the GDPR. The other dimension of this is being able to demonstrate this compliance. This will involve keeping records of data processing activities and to ensure that your organisation is able to show the Information Commissioner’s Office (ICO) that it is compliant with the GDPR.  Compliance will require the entire organisation to get involved and one of the essential but simple steps that you can be taking now to ensure compliance is to raise awareness in your organisation. Training all staff on the GDPR and your requirements to comply is key, but especially those who make major decisions or deal with personal data as part of their role. Board-level buy-in is essential and will ensure that compliance with the GDPR is a top-to-bottom priority in your company.  You might want to consider the appointment of privacy champions in each department. These would be advocates of good data protection and privacy practices and provide individual departments with initial advice on data protection queries. The privacy champions should be familiar with data protection processes, policies and escalation routes.   1. **Data Protection Officers**   Data controllers and data processors need to consider whether they need to appoint a Data Protection Officer (DPO). Data controllers and processers must appoint a DPO in the following circumstances:   1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; 2. the core activities of the data controller or data processor consist of processing which requires regular and systematic monitoring of data subjects on a large scale; or 3. the core activities of the data controller or data processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.   The DPO has a number of tasks outlined in the GDPR and businesses may wish to consider setting up a DPO team to support the role. Even if you don’t meet any of these thresholds set out in Article 37, you may wish to consider appointing a DPO to assist with your GDPR compliance.   1. **Internal reviews**   Many data controllers and data processors are carrying out internal reviews or audits of the personal data that they deal with in order to examine current practices and policies and assess them for GDPR-compliant updates. This is usually done in the following phases:  **Phase 1: Management buy-in**   * Secure your resources/budget and discuss DPO requirements.   **Phase 2: Fact finding**   * Fact finding and interviews with employees. * Gathering evidence in the form of policies, procedures, training modules etc.   **Phase 3: Gap analysis and to-do list**   * Review all the responses. * Create a to-do list. * Identify risk areas for development and create a strategy to achieve full compliance in the light of these.  1. **Data protection by design and DPIAs**   The concept of data protection by design and default requires data controllers and data processors to consider data protection rights in all of its processing activities and to implement appropriate technical and organisational measures to ensure that those rights are safeguarded.  Data controllers and data processors should begin to think about this now and start integrating data protection into your day to day business activities and when they are introducing new systems or designing new products for their business. They should also consider the use of Data Protection Impact Assessments (DPIA), understand what a DPIA is, when they need to be carried out and how they will go about this. The Article 29 Working Party (the group of EU regulators) has provided detailed guidelines on DPIAs, which are available [here.](file:///C:\Users\567\Downloads\wp248_enpdf.pdf)   1. **Consent**   Under both the current data laws and the GDPR you must have a lawful ground under whichto process personal data in order for your processing to be fair and lawful. One such reason is consent obtained from the data subject, and there are strengthened requirements to obtain adequate consent under the GDPR. Consent must be a ‘*freely given, specific, informed and unambiguous indication’* of an individual’s wish ‘*by a clear affirmative act’* indicating their agreement to the processing of their personal data, and under the GDPR the notice provided to the individual when consent is being sought must be:   * Clearly distinguishable; * Easily accessible; and * In clear and plain language.   Consent must not be conditional on other matters and must also be as easy to withdraw as to give. This means that pre-ticked boxes, silence or inactivity will not be sufficient and information in relation to the consent being sought cannot be buried in lengthy, dense privacy policies. Data controllers and data processors must be able to demonstrate that they have obtained consent and should therefore record the consent obtained.   1. **Privacy notices**   The GDPR requires data controllers to provide data subjects with concise, transparent, intelligible and clear information about the ways in which they use their information (through the use of privacy policies, privacy notices etc.) and minimum information must be provided to the data subjects at the point at which the data is collected or, if data is collected via a third party, within a reasonable period after obtaining the information. One step that you can take immediately is to review your privacy policy, review the notices that are provided on your website and check your marketing consents for compliance.   1. **Individual rights and subject access requests**   The GDPR strengthens the rights of data subjects and introduces certain new rights, such as:   * The right to have personal data erased; * The right to restrict processing of personal data; and * The right to data portability.   Data controllers and data processors should plan now how they will deal with requests from data subjects who wish to exercise these rights, and put policies and procedures in place to deal with them.  The timescale for responding to a data subject access request (DSAR) has been reduced from 40 days to 1 month and you should plan how you will deal with such requests in advance of the GDPR. It might be helpful to carry out a data mapping exercise to identify where personal data is being held and for what purpose. Organisations will need to be ready for a potential increased number of DSARs and have a procedure which makes it easy to respond promptly.   1. **Review arrangements with third parties**   Data controller-data processor relationships are much more regulated under the GDPR and data controllers are obliged to engage data processors which provide certain guarantees in relation to GDPR compliance. The processing by the data processor will have to be covered by a written contract which sets out certain prescribed terms. Unfortunately there are no exemptions for data processing agreements that are already in place so you need to update your data processor clauses and agreements before 25 May 2018.  In order to prepare for these changes, you should review and update data processor clauses in supplier agreements. For contracts that are already in place, providing the new clauses to processors in an addendum to the current contract is a good way to avoid opening up negotiations in other areas of the contract.   1. **Data breaches**   For the first time in the UK, there is a requirement to notify the ICO and data subjects that a data breach has occurred in particular circumstances. You will have just 72 hours after becoming aware of a data breach to notify the ICO unless the breach is unlikely to result in a risk to the rights and freedoms of the data subjects affected. You must notify data subjects that a breach has occurred without undue delay if there is a high risk to their rights and freedoms. Due to the time restraints, it would be sensible to put a plan in place for reacting to a data breach and to have a ‘dry run’ to practice how to respond in case a data breach occurs.  Under the GDPR, you are required to keep records of data breached and, even if the breach does not need to be reported, the controller should still record:   * The breach; * The facts relating to the breach; * Its effects; and * Remedial action taken.  1. **International transfer of data**   One of the big changes to EU data protection law under the GDPR is its extra-territorial scope. It applies to data controllers and data processors established outside EU but processing personal data of individuals in the EU where the processing activities are related to:   * offering goods or services in EU; or * monitoring behaviour in EU.   To ensure compliance, organisations should assess where their data is being processed, ensure that any branch offices outside the EU are GDPR-ready and check that they have appropriate safeguards in place. Organisations may also need to update their privacy policies to be transparent about where personal data is being transferred.  **Grandfathering**  Finally, an important point to note during the preparation process is that the GDPR has no provision for ‘grandfathering’; the new rules apply to old data. For example, you might need to obtain new consents as it is unlikely that consent obtained under the current regime will be compliant with the GDPR. |  | BUSINESS CONTACTS **Nicola Barden**  Associate  [nicola.barden@harbottle.com](mailto:nicola.barden@harbottle.com) |