10 STEPS TO TAKE TOWARDS GDPR COMPLIANCE

STEP 1

Carry out a data audit!

Document what personal data you hold, where it came from, why was it originally gathered, how long you will retain it, how secure is it and who you share it with – so that if you hold inaccurate information you will know this and be able to rectify it. You should identify (and document) the basis (under law) for your processing personal data (eg processing is based on consent or processing is necessary to perform a contract) as some individuals rights will be modified depending on your lawful basis for processing their personal data. For example, individuals have a stronger right to have their data deleted where consent is used as the lawful basis for processing.

STEP 2

Review privacy policies

Review your privacy policies in order to address the additional information requirements that are necessary under the GDPR. Information must be provided in concise, easy to understand and clear language.

STEP 3

Review your plan for dealing with access requests

Review procedures to ensure that they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format, if requested. Consider and plan how you will deal with requests from individuals (eg seeking access or deletion of their data). The timescale for processing requests have been shortened from 40 days to one month. If you handle a large volume of access requests, you should consider the logistical implications of having to deal with requests more quickly.

STEP 4

Review how you seek, record and manage consent

Review how you seek, record and manage consent and whether you need to make any changes to this process. You are not required to refresh all existing consents in preparation for the GDPR, but if you rely on consent to process personal data, you should ensure that it meets the GDPR standard on being freely given, specific, informed, unambiguous and in plain language. If not, alter your consent procedures and seek fresh GDPR-compliant consent or find an alternative basis under the GDPR for processing personal data.

STEP 5

Consider children and consent

In relation to children, consider whether you need to put systems in place to verify individuals' ages and to obtain parental / guardian consent for any data processing activity. If you offer online services to children and rely on consent to collect information about them, then you may need consent from a parent / guardian in order to process the child's personal data lawfully. The consent has to be verifiable and your privacy notice must be written in language that children will understand.

Maureen Daly, partner and head of data protection
Riverside Two, Sir John Rogerson's Quay, Dublin 2, Ireland. **T:** +353 1 418 0912 **E:** m.daly@beauchamps.ie

BEAUCHAMPS

10 STEPS TO TAKE TOWARDS GDPR COMPLIANCE

STEP 6

Consider if you need to appoint a DPO

Consider whether you need to appoint a DPO. Even if you conclude that you do not need to appoint a DPO under the GDPR, you should still identify a person who is responsible for the organisation's data protection compliance, careful not to designate that person as a DPO which would result in GDPR compliance requirements.

STEP 7

Review and update data breach procedures

Review procedures to ensure that you will be able to detect, report and investigate personal data breaches. You should have an incident response procedure in place in the event of a personal data breach and have a clear plan of action and ensure it is implemented and tested as it will need to be live by 25 May 2018.

STEP 8

Remember your employees and your suppliers

Your employees should be made fully aware of the implication of the changes and should be trained in the application of any new policies. DPIAs may need to be conducted if required and measures should be adopted to mitigate risk.

Review your arrangements with suppliers as it may be necessary to make contractual amendments in order to comply with the GDPR.

STEP 9

Start keeping records of your data processing activities

You will also need to keep a record of data processing activities which must be provided it to the DPA, on request, to demonstrate compliance.

STEP 10

Consider the international element, if necessary

If your business operates in more than one EU Member State, you should map out where your business makes its most significant decisions about its data processing activities. This will help to determine your 'main establishment' and therefore your LSA. This should be documented.

Maureen Daly, partner and head of data protection
Riverside Two, Sir John Rogerson's Quay, Dublin 2, Ireland. **T:** +353 1 418 0912 **E:** m.daly@beauchamps.ie

BEAUCHAMPS