Preparing for the law enforcement requirements (part 3) of the Data Protection Bill: 12 steps to take now

1

Awareness

Check if you are a Competent Authority under Schedule 7 of the DP Bill or have statutory functions for any of the law enforcement purposes. If so, you should make sure that key people in your organisation are aware that the law is changing from May 2018.

2

Information you hold – mapping

You should document what personal data you hold, where you hold it, where it came from, who you share it with and who is responsible for it. Identify what personal data is being processed under Part 3 (of the DP Bill) and what is being processed under other parts of the Bill and GDPR. Do you work jointly with other organisations? Do you use data processors? You may need to organise an information audit and review any contracts or agreements.

3

Lawful basis for processing personal data

You should identify the lawful basis for your processing activity, document it and update your privacy notices to explain it, using clear and plain language.

4

Consent

If you rely on consent you need to consider whether this is appropriate or whether you should use another lawful basis. If consent is appropriate then you should review how you seek, record and manage consent and whether you need to make any changes. You will need to refresh existing consents if they do not meet the standard required.

5

Privacy notices

You should review your current privacy notices and ensure that these are in an easily accessible form, updated and are ready by May 2018. You will need to include more detailed information including your lawful basis for processing personal data and retention periods unless an exemption applies.

6

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals may have, including deletion, so that you know how you will respond within the specified timescales.

ico.
Information Commissioner's Office

ico.org.uk

7

Data breaches

You should ensure that you have the right procedures in place to identify, manage and investigate a breach. You will need to have processes in place to determine whether you need to report the breach to the ICO, based on the risks to individuals' rights and freedoms. If you decide that it is necessary to report you will need to do so no later than 72 hours after becoming aware of it. You should be prepared to notify affected individuals in some cases.

8

Data protection by design and DPIAs

Make sure you are familiar with the ICO's code of practice on privacy impact assessments as Data Protection Impact Assessments will be mandatory where any processing is likely to result in a high risk to the rights and freedoms of individuals.

9

Data Protection Officers

Ensure you designate someone to take responsibility for your data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You will be required to have a Data Protection Officer (unless you already have one under the requirements of the GDPR or a specific piece of European law enforcement legislation).

10

Logging

You should ensure that you are able to keep logs of processing operations in automated processing systems. This will include a log of any alterations to records, access to records, erasure and disclosures of records unless an exemption applies.

11

International

You should review procedures for transferring or sharing personal data across borders (either with relevant authorities or others) to ensure that they are compliant.

12

Sensitive processing

If you are undertaking sensitive processing you will need to ensure that you are compliant with the requirements of the legislation including having an appropriate policy in place.