HRC Law

TEAM SERVICE PROVIDER

Is your business GDPR compliant?

The **GDPR** or **General Data Protection Regulations** to give it it's full title, is a piece of data protection legislation that came into force on the 25th May 2018.

Now that this new legislation is in force, you should ensure that the ways in which you deal with personal data in your business are compliant with it.

What has changed?

Consent

Businesses can no longer rely on 'implied consent'. This means that you can't continue to use tick boxes that are already ticked when obtaining an individual's consent to use their personal data.

Since May 2018 you must be able to demonstrate clear specific, unambiguous and informed consent from the individual (data subject) who provides a clear affirmative statement or action which is easily able to be withdrawn.

Continuing to require an individual to untick a box, will almost certainly breach the GDPR. Obtaining effective consent will be much harder.

You've hopefully already reviewed your forms and consent processes to make sure that any changes necessary are planned and budgeted. If you haven't, and you need support, please get in touch.

The GDPR requires explicit and continuous consent from individuals. This means that you are required to keep detailed records of continual reviews of your data processes (required by the GDPR) and if this does not already set your hares running, you are also required to delete data which is not being kept for a specific purpose.

If you ever deal with children between the ages of 13 & 16 you are also now required to obtain parents' consent (in the same way as described above) to use the personal data lawfully.

Territory

Many businesses are affected by the GDPR and in turn could be in breach without knowing it! Whether based in Manchester, California or Japan, if your business either: (i) offers goods and/or services to data subjects in the EU (irrespective of whether payment is received), and/or (ii) monitors data subject's behaviour which takes place within the EU, your business will be subject to the GDPR.

Data Protection by Design

GDPR requires data protection to be embedded in the entire life-cycle of a project or process, from the early design stage, continuing through to its ultimate deployment, its use and final disposal. This principle is expected to be used when your business is creating services or products or if your business is data heavy, any data processing activities. GDPR requires businesses to perform data protection

impact assessments before carrying out any processing that uses technology, this will include anything that is high risk such as the use of job boards (where individuals are using automated processing or profiling), created by your business or using a third party's technology. This may require measures such as pseudonymising (processing personal data in such a manner that the personal data cannot be attributed to a specific individual) or ensuring that the third party who supplies the technology complies with the GDPR.

The Right to be forgotten

Data subjects have the right to be erased from a business's database. This requires a streamlined process following a data subject's request to be erased. If your business is holding personal data that is not intended for the purpose given by the individual, your business will be required to delete it (or obtain their consent to use it for such a purpose). A data subject has the right to object to their personal data being processed (such as online tracking and behavioural advertising). This requires businesses that use these mechanisms to obtain consent for these types of activities.

Mandatory Notification of Data Breaches

It is now mandatory to report all breaches of data protection to the Information Commissioner within at least 72 hours of becoming aware of the breach under GDPR, unless the breach is unlikely to result in risk for the rights and freedoms of individuals. In the past reporting a breach was only voluntary. Now, your current policies and processes should be compliant with the reporting requirements, including educating employees in relation to them. Remember that GDPR also impacts on data processors as they may be liable to pay fines if they do not comply with their obligations, whereas they were not subject to obligations under the DPA.

Mandatory Data Protection Officers

Businesses whose core activities consist of processing sensitive data or require regular and systematic monitoring of data subjects, are now required to formally appoint a Data Protection Officer. Sensitive personal data has been widened by GDPR to include retinal scans and fingerprints in order to keep up with developing technology.

Data Subject Access Requests

Businesses are obliged to reply to data subject access requests within one month from the date of receipt of the request. If you receive requests on a regular basis, you should have incorporated these new timescales into your processes.

What are the consequences of breaching GDPR?

Non-compliance with the GDPR has significantly increased the risk to your business. The position under the old data protection law was that the UK could fine a business up to a maximum of £500,000 for breach of data protection laws.

The GDPR has created a new level of substantial fines on data processors and data controllers in two areas (it only used to be data controllers that were obliged to comply):

(i) up to 2% of annual worldwide turnover of the preceding financial year or 10 million euros (whichever the greater) for violations relating to internal record keeping, data processor contracts, data security & breach notification, data protection officers and data protection by design and default; and

(ii) up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros (whichever the greater) for violations relating to breaches of the data protection principles, conditions for consent, data subjects' rights and international data transfers.

General

Under the new accountability principle, the GDPR requires businesses to continually look at the degree of risk that their current processes may pose to data subjects. This requires time to implement. A failure to plan ahead could leave businesses struggling to remain compliant with the GDPR.

If you would like to be invited to our training workshops or need help amending contracts or streamlining processes please contact us on 0161 358 0545 or simonwhitehead@hrclaw.co.uk

HRC Law LLP
Acresfield
8-10 Exchange Street
Manchester
M2 7HA