Wellers Law Group LLP

April 2017

Briefing Note

General Data Protection Regulation 2016 (GDPR)

NEW DATA PROTECTION RULES – ARE YOU READY OR AT RISK OF HUGE FINES?

New tougher data protection rules are going to apply to every organisation in May 2018 – so why the urgency from UK regulators insisting that organisations need to prepare for them now?

Prepared by: Jennifer O'Brien, Wellers Law Group LLP
jennifer.obrien@wellerslawgroup.com or on 020 7481 6383.

Wellers Law Group LLP is registered in England and Wales, registered number OC350170 and is authorised and regulated by the Solicitors Regulation Authority No 525515.

What is happening?

The new rules are much tougher than the existing rules in many ways which means that even if you comply with the current regime (or don't!) you will have to review what you do with data and take action to make sure you comply with the new rules in time.

Notable areas of change are:

- Obtaining consent - consent for use of individuals' data will be more difficult to obtain – organisations will have to be able to prove 'unambiguous agreement' to use of data
- Accountability – this new concept means that organisations will have to be able to demonstrate/prove compliance with the new regime by multiple means including implementing policies, training and record keeping
- Provide customers with more information - individuals must be provided with even more information than is currently the case about use of their data by an organisation called an 'information notice'
- Data protection by design – another new concept which means that whenever an organisation adopts a new technology, product or service data protection compliance needs to be considered from the outset
- Wider application - the GDPR will apply to data processors (i.e. those who process data on the instructions of data controllers) as well as data controllers – a significant change!
- Data Protection Officer - many organisations will need to appoint a Data Protection Officer
- Data breaches - these will need to be reported to the regulator and individuals affected (every organisation's nightmare) – this could lead to heavy fines and serious reputational damage!

If all of that wasn't enough GDPR will apply not only to EU member states but also to entities outside the EU if their activities involve offering goods or services to EU data subjects.

What is the law?

The new rules are called the General Data Protection Regulation 2016 (GDPR). Essentially they govern how organisations handle personal data i.e. information which identifies an individual. They will replace the current regime (the Data Protection Act 1998) from May 2018.

Why is it changing?

Technology has developed rapidly since the existing laws were introduced – just consider the development of the world of tablets, apps, social media which were almost 'unknowns' when the original rules came into force. Over time EU authorities have recognised that the current regime did not provide an adequate framework for protection of individuals' rights regarding use of their data by organisations particularly given the exponential increase in use of data by organisations. The new regime therefore aims to provide that protection, taking account of various technological advances, but most significantly increasing the level of fines for breach to such a degree that organisations are effectively compelled to take data compliance more seriously (or risk costly penalties and serious reputational damage if they do not).

Who is affected?

No matter what kind of organisation you are (corporate/charity/small business/sole trader) the changes will apply to you. As also stated above the new rules have wider application as they will apply directly to data processors as well as data controllers.

Are there any benefits?

Yes! Many of the existing principles are retained in the GDPR so in some instances it will be a case of continuing to do the same or simply doing it to a higher standard. One shouldn't forget either that good data use can add value to a business – not only increasing operational efficiency and reducing the risk of breaches but encouraging customer/public confidence in an organisation thereby leading to increased profitability.

What are the risks to your organisation?

The new rules essentially aim to create a cultural change in the way in which data is controlled and used by organisations with a view to protecting the privacy rights of consumers. It applies to all kinds of data held by organisations and almost every action an organisation carries out relating to that data.

On a practical level there are three reasons why complying with the GDPR is urgent:

One, because the rules introduce lots of new 'must do's'. If anything ever goes wrong with your data (like a cyber-attack leak which is not unlikely) you have to be able to prove to the regulator that you've taken steps to prevent that happening. Many organisations can't;

Two, because the fines for failing to comply with the new rules are potentially huge. They are increased from the current maximum of £500,000 to up to 4% of annual worldwide turnover or €20m (for serious breaches) – 40 times higher than the current regime! So data protection compliance is now a major risk for organisations which they ignore at their peril;

Three, because a failure to comply with the regime can lead to catastrophic reputational damage and loss of consumer confidence in an entity be it charitable or corporate!

What mitigation/action is needed?

The good news is that it isn't too late to prepare for the new rules but yes, you need to begin immediately as there is a lot to change as well as put in place for the first time.

The easiest approach is to carry out a data protection audit or health-check – that means identifying what you do with data now and what you need to do to get your house in order in time.

We are specialists in this area and can help. We can also customise a health-check product for you so you get a clear idea of cost from the beginning, ranging from a basic audit (at lower cost) to products that go a little deeper (giving your organisation greater reassurance with some additional cost) but all of which will be helpful in mitigating against future heavy fines.

Next steps

For further assistance please contact Jennifer O'Brien at jennifer.obrien@wellerslawgroup.com or on 020 7481 6383.