

9 July 2017

insider.co.uk

10 significant changes to data protection law under GDPR which businesses need to plan for right now

Laura Irvine of BTO - one of the panel members at Insider's Cyber Security Business Breakfast next month - outlines why firms must start planning now for the General Data Protection Regulation shake-up in May next year



BY PHILIP GATES
12:18, 9 JUL 2017



It's feared many businesses are not preparing properly for GDPR

It's been labelled the biggest shake-up of data protection law in a generation.

The General Data Protection Regulation, or GDPR, will come into force in May 2018.

But how will it really affect business? Insider is holding a [Cyber Security Business Breakfast](#) on August 24 on what GDPR means for your organisation.

[Scott Simpson, founder of The Security Circle, is keynote speaker at Insider's Cyber Security Breakfast](#)

Ahead of that breakfast [one of our panel members](#), BTO's Laura Irvine, outlines 10 steps that business must look out for. Here they are:

The General Data Protection Regulation (GDPR) will have direct effect throughout Europe from 25 May 2018.

The UK will still be in Europe at that time. The Government has confirmed that UK businesses will need to comply. Post-Brexit there are unlikely to be many changes as the GDPR standards are likely to remain the same to allow the UK to do business with Europe.

1. Lawful Processing and Consent

It will become much more difficult to obtain valid consent under the GDPR but there are other lawful bases which have been ignored under the DPA.

Businesses must identify what lawful basis it is relying on: is it necessary for you to gather the data for the performance of a contract; is it necessary for you to share the data because of a legitimate interest you have?

2. Transparency and Fair Processing

Any processing must also be done fairly which means telling individuals what you are doing with their data even if you do not require their consent.

Under the GDPR you must provide the following information in a Privacy Notice when you collect their information:

your identity;

the purpose for processing;

the legal basis for processing;

the categories of personal data concerned;

the recipients of personal data if any; and the safeguards in place if data is to be transferred to a country outwith the EU.

Other information must also be made available such as the how long you will keep the data and a list of the rights each data subject has.

READ MORE

► Cyber Security Business Breakfast - 24th August

3. Data Protection by Design and Data Privacy Impact Assessments

For any new project if there is likely to be a high risk to the privacy rights of individuals then a Design and Data Privacy Impact Assessment (DPIA) should be carried out and in particular this refers to large scale processing of sensitive data; systematic monitoring of a public area and automated processing where the decisions have a legal or significant impact on individuals.

4. Accountability and Recording Data Processing

If you have over 250 employees or your processing is likely to result in a risk to the privacy rights of individuals then you must maintain a record of processing including the purpose of your processing; the categories of data you are processing; the recipients of data including if they are in a third country.

5. Data Protection Officer

Certain organisations will require to have a DPO to advice on GDPR compliance. This individual cannot be someone who makes decisions about data processing but should have access to the

Certain organisations will require to have a DPO to advice on GDPR compliance. This individual cannot be someone who makes decisions about data processing but should have access to the Board.

The responsibility remains with the data controller; the organisation in control of the data. If you are a public authority; if you're core activity is processing large amounts of sensitive personal data or if you're core activity involves systematic monitoring, then you must have a DPO.



6. Data Subject's Rights

There are some enhanced and some new rights and organisations must have a system in place to deal with them. The timescales are tight for compliance. Subject access requests must be complied with in 30 days.

In certain circumstances there is a right to be forgotten; a right to restrict processing and a right to object to processing. There are new rights concerning automated decision making and a right to move your data from one provider to another – data portability.

7. Children

If you are processing the data of children you must decide whether you need to have a system in place to confirm their age and to obtain parental /guardian consent if you are offering online services.

Information provided to a child should be in an easily understood format. Under the GDPR a child is defined as under 16 however the UK may reduce that age to under 13.

8. Data Controllers and Data Processors

Both now have obligations to comply with the law and both can be investigated and fined.

Any contract a data controller has with a processor must contain certain terms set out in the Regulation to ensure compliance and to ensure that the controller is aware of any sub-contractors.

9. Personal Data Breaches

A personal data breach must be reported to ICO without undue delay and within 72 if it being discovered unless there is likely to be no risk to the privacy rights of any individual.

If there a high risk to the privacy rights of individuals then they must also be notified without undue delay.

10. ICO Powers

The ICO will have the power to impose significantly increased levels of fines up to a maximum of €20 million or 4% of global turnover, whichever is higher for processing breaches (not just personal data breaches), and €10 million or 2% global turnover for the more administrative breaches.

Laura Irvine is Associate and Solicitor Advocate for BTO Solicitors LLP