What employers should know about the new General Data Protection Regulation

[et_pb_section admin_label=”Section” global_module=”136″ fullwidth=”on” specialty=”off” transparent_background=”off” background_color=”#ffffff” allow_player_pause=”off” inner_shadow=”off” parallax=”off” parallax_method=”off” padding_mobile=”off” make_fullwidth=”off” use_custom_width=”off” width_unit=”on” make_equal=”off” use_custom_gutter=”off”][et_pb_fullwidth_code global_parent=”136″ admin_label=”Post Header”][Page_Header_Start] Employment Law News[Page_Header_End][/et_pb_fullwidth_code][/et_pb_section][et_pb_section admin_label=”section”][et_pb_row admin_label=”row”][et_pb_column type=”3_4″][et_pb_text admin_label=”Text” background_layout=”light” text_orientation=”left” use_border_color=”off” border_color=”#ffffff” border_style=”solid”]

What employers should know about the new General Data Protection Regulation

[post_details]

[Social-Share]

The Government has confirmed that the UK will implement the General Data Protection Regulation in May 2018. Though amendments may be made once the UK leaves the EU, employers should start making preparations now.

Whilst the UK voted to leave Europe in the 2016 referendum, on the Government's timetable the UK will still be in the EU when the GDPR comes into force on 25 May 2018. The penalties for non-compliance can be very serious; data controllers could be fined up to €20 million or 4% of annual worldwide turnover. Therefore, there is good reason for employers to plan ahead.

Giving notice

As the Information Commissioner recognised, the GDPR gives "people greater control of their data".

Specifically, employers need to be more transparent about how they use personal data and give employees more information about their processes. Included within that is a requirement that employers must give fuller 'fair processing notices'.

The notices need to say in clear and concise language: (i) who the data controller and Data Protection Officer are and how to contact them; (ii) why personal data is being processed; (iii) what legitimate interest there is in processing personal data; (iv) who will receive the personal data; and (v) if the data will be transferred outside of the EEA (and if so, where).

At the point where an employer collects personal data from an employee or job applicant, another notice needs to be given to make clear: (i) how long the data will be retained for; (ii) the right to have their data deleted or modified; (iii) the right to withdraw consent to the data being processed; (iv) the right to complain to the Information Commissioner; (v) the consequences of the employee or applicant not giving the data (i.e. if there is a contractual or statutory requirement for them to do so); and (vi) if the data will be used for automated decision-making.
Employers have an obligation to ensure that their employees are aware of these details, so the best approach would be to have a separate document (i.e. not a section squirreled away in a handbook) which you ask the employee or candidate to read.

Getting consent

Having an employee or applicant's consent is one way to process their data lawfully. However, consent under the GDPR needs to be "freely given, specific, informed and unambiguous". That means that pre-ticked tick boxes or opt outs will not suffice.

Rather than including a term in employment contracts, employers should provide all the relevant information about data processing in a separate consent form for employees to sign up to. This places less pressure on new and existing employees and lends itself to the argument that consent was freely given.

However, there are murmurs in the EU as to whether consent can ever be freely given in an employment relationship given that employees have less bargaining power than their employers. That being so, it is worth ensuring that one of the other reasons for processing data is present. They are where processing is necessary for:

- performance of a contract;
- compliance with legal obligations;
- protection of the data subject's interests;
- tasks in the public interest; or
- the data controller's legitimate interests.

In addition to writing to the employee with information about data processing, employers should have a clear policy on data protection. Employers also need to ensure that it is accessible to all staff and that they are aware of it.

Data systems

Data subjects will have the right to ask employers to delete or modify personal data held about them. Therefore, it is important that employers' IT systems are capable of managing data easily and efficiently. It should be possible to delete

data from them permanently and to place restrictions on who can access it.

Employers will also need to know how long data is stored under their system before it is automatically deleted (assuming that it is).

Data security breaches will be treated severely, so employers should ensure that data held is encrypted and kept securely. There should also be a mechanism for employers to be alerted when a breach has taken place, as there is a 72-hour deadline in which to notify the Information Commissioner.

Most employers will be familiar with the rules on data subject access requests as they stand, but the GDPR will bring changes. The deadline for response to a DSAR will be cut down to one month rather than the previous 40-day timeframe (though it can be extended to two months when necessary, employers should always aim for the shorter deadline to be on the safe side). The requirement for a fee to be paid will also be removed.

In order to ensure compliance, employers should check that their systems will permit them to complete a search within the month’s deadline; in larger companies, it may speed the process along to appoint someone specific to deal with DSARs as and when they come in.

Fundamentally, May 2018 is not as far away as it seems, particularly where changes to IT systems or HR procedures are required.

Employers should therefore start to review their systems and schedule any changes which may be necessary.

Even if Brexit happens, Parliament is unlikely to make meaningful changes to data protection laws. To do so would impede trade by conflicting with the EU’s strict rules about transferring data to countries without adequate protection.

[/et_pb_text][/et_pb_column][et_pb_column type=”1_4″][et_pb_sidebar admin_label=”Sidebar” orientation=”right” area=”sidebar-1″ background_layout=”light” remove_border=”off”] [/et_pb_sidebar][/et_pb_column][/et_pb_row][/et_pb_section][et_pb_section admin_label=”section”][et_pb_row admin_label=”row”][/et_pb_row][/et_pb_section]