CLIFFORD

CHANCE

THE GENERAL DATA PROTECTION REGULATION: IMPLICATIONS FOR EMPLOYERS

On 25th May 2018 the General Data Protection Regulation (the "**GDPR**") will have direct effect in the UK replacing the current Data Protection Act 1998 ("**DPA**").

Although many of the principles and rules in the GDPR are similar to, or the same as, those in the DPA, there are new rules which will require some changes in approach by employers as data controllers. This Briefing examines how the GDPR will impact on current employment practices, what employers will have to do differently and what will no longer be possible.

Key issues

- What is the legal basis for processing the personal data of staff?
- Relying on consent: what needs to change?
- Accountability: demonstrable compliance, data privacy notice and more
- Subject access requests do current arrangements require revision?
- Do you need a data protection officer?
- International transfers of staff data
- Penalties for breach
- Action points

What is the legal basis for processing the personal data of staff?

Employers must have a legal basis for processing the personal data of their staff (whether employees, contractors or otherwise); this must be set out in their privacy notices (see below) and in response to a subject access request. At present some employers rely on consent to justify their data processing; relying on consent has always been slightly uncertain but under the GDPR it is highly unlikely to provide the legal basis for processing the personal data of staff. The Information Commissioner's Office (the "ICO") recommendation is that employers should avoid relying on consent, and instead rely on one of the other processing conditions set out in the GDPR such as performance of the contract or compliance with a legal obligation.

Action:

Employers should consider if they should rely on one of the other processing conditions in the GDPR.

Relying on consent: what needs to change?

It will in some circumstances still be possible for employers to rely on consent to justify their data processing. If employers do intend to rely on 'consent' the GDPR requires this to be freely given, specific, informed and unambiguous. An employer must be able to demonstrate that consent was given; clear audit trails will be required. An employer will not be able to infer consent from silence, a pre-ticked boxed or inactivity. Employers who intend to continue relying on existing consent mechanisms should verify that they meet the GDPR requirements.

Accountability: demonstrable compliance, data privacy notices and more

The GDPR introduces a new principle of accountability: employers as data controllers will have to demonstrate how the GDPR has been complied with; technical and organisational measures including thorough policies, processes; employee training and extensive record keeping are all likely to be required.

At present employers (as data controllers) are required to provide concise, transparent and easily accessible information on: the identity of the controller, (i.e. the employer), the purposes for which it is being processed, and additional information necessary to be able to process the information fairly. As part of this GDPR accountability principle employers are likely to have to revise their data privacy notices (or equivalent documentation) to include more information.

The GDPR requires additional information to be provided in the data privacy notice including the data subject's rights to withdraw consent, to lodge a complaint with the data protection authority (i.e. the ICO in the UK), access to, rectification and erasure of data, and the existence of any automated decision making (e.g. profiling as part of a recruitment process).

Action:

Employers should audit existing arrangements to assess what revisions need to be made to their data privacy notices and whether procedures are in place to make them available at the appropriate point in the employment cycle.

The GDPR will also require employers to notify the ICO of any data protection breach without undue delay and in any event not later than 72 hours after having become aware of it unless the controller can demonstrate that the breach is unlikely to result in a risk to the data subject . The data subject must also be notified of the breach without undue delay. In principle this could cover situations where a laptop with unencrypted HR data is lost or an email with staff sickness absence data is sent to the wrong recipient.

Action:

Employers should update their data protection policies and procedures to ensure these new notification requirements are embedded.

Subject access requests ("SARs"): do current arrangements require revision?

At present an employer has 40 days to respond to a SAR. The GDPR reduces the response period to one month. The response time may be extended by two further months where necessary taking into account the complexity and number of the requests. There will be different grounds for refusing to comply – manifestly unfounded or excessive requests can be charged for or refused.

Employers will be required to provide additional information in the SAR response; this includes details of the individual's rights to be forgotten, to rectification of inaccurate data and to restrict the processing of their data (the 'delete it, freeze it and correct it' rights).

Action:

Employers should update their internal templates to ensure SAR responses comply with the new requirements and ensure staff dealing with SARS's are aware of the new requirements.

Do you need a data protection officer?

Public authorities and organisations whose activities will involve processing of sensitive personal data on a large scale, or, which by virtue of the nature of their activities will regularly monitor data subjects on a large scale will be required to appoint a data protection officer ("DPO"). The DPO will have the right not to be dismissed or subject to a detriment for performing their role. In some member states it will be compulsory to have a DPO.

Organisations can voluntarily appoint a DPO, however, should they do so the DPO will be eligible for the same protection against dismissal or detrimental treatment.

Action:

Employers should consider if they need to appoint a DPO.

International transfers of staff data

Under the GDPR it will still be possible to transfer staff personal data to countries outside the EEA which ensure "adequate" protection for personal data, however, the GDPR does not permit data controllers to reach their own view on the adequacy of the regime. Unless the country is on the EC's approved list of countries it will be assumed not to be adequate.

Once Brexit is complete this may be problematic for multi-national employers wishing to send employee data to the UK from elsewhere in Europe if the UK is not on the list of approved countries; and it is thought that post Brexit the UK will not be regarded by the European Commission as an "adequate" country. Unless a special exception is agreed transfers of personal data from the EU to the UK will be prohibited unless standard form data transfer agreements or binding corporate rules are relied upon in such circumstances.

Penalties for breach

At present the ICO can impose a financial penalty of up to £500,000 for breach of the DPA. The GDPR provides for fines for serious breaches of the GDPR up to the higher of 20,000,000 Euros or 4% of the group global turnover for the preceding financial year. For less serious breaches fines will be up to the higher of 10,000,000 Euros or 2% of the group global turnover. As at present individuals will be able to claim compensation through the civil courts for damage or distress suffered as a result of breaches.

Additional Action points

- Appoint an individual or group to be responsible for undertaking a review and update of the company's employment policies, procedures and practices in relation to staff data.
- Identify what 'staff' data is processed and its source.
- Audit existing arrangements to assess the extent to which consent is relied upon as the basis for processing staff data (if at all).
- Identify/establish the lawful basis for processing staff data from May 2018.
- If consent is to be relied upon consider whether mechanisms need to be revised in application forms, contracts and elsewhere.
- Audit recruitment materials, employment contracts, staff handbooks, intranet pages, and other policies and procedures to assess whether privacy notice wording needs to be revised to meet GDPR requirements.

- Review policies and response procedures in relation to subject access requests to ensure that the new one month timeframe can be met.
- Consider how personal data can be readily accessed and removed, corrected or its use restricted, where data subjects exercise their 'delete it, freeze it, correct it' rights or the business interests for which it was processed have ceased.
- Assess whether a data protection officer has to be appointed, or if not, whether it is nevertheless a good idea to do so.
- Identify what staff data is transferred outside the EEA and assess if it is covered by a GDPR compliant transfer mechanism.
- Consider the impact of Brexit on staff data transfers to the UK.
- Consider what staff training is required for those staff involved in the processing of personal data.
- Keep an eye out for guidance and advice from the ICO office at www.ico.org.uk.

[Clifford Chance has an extensive global team of employment and data protection lawyers who have supported clients in relation to the issues arising from the GDPR.]

CONTACTS

Chris Goodwill
Partner

T +44 207 006 8304
E chris.goodwill@cliffordchance.com

Mike Crossan
Partner

T +44 207 006 8286
E michael.crossan@cliffordchance.com

Alistair Woodland
Partner

T +44 207 006 8936
E alistair.woodland@cliffordchance.com

Chinwe Odimba-Chapman
Senior Associate

T +44 207 006 2406
E chinwe.odbima-chapman@cliffordchance.com

Tania Stevenson
Senior PSL

T +44 207 006 8938
E tania.stevenson@cliffordchance.com