Information Security and Data Protection Newsletter - March 2016

Published 1 March 2016

New EU Data Protection Regime: What are the implications for employers as data controllers?

Previous alerts have covered the broader aspects of the GDPR. In this month's editorial, as we approach the formal adoption of the GDPR, Khurram Shamsee, employment and data protection specialist, focuses on some of the key implications of the GDPR for employers as data controllers.

The headline is that the GDPR is unlikely to mark a sea-change for how organisations handle the personal data of their employees, ex-employees, job applicants and contractors. Indeed the GDPR may well lead to a divergence in how organisations deal with employee personal data, as compared to the data of customers, consumers and other data subjects.

From an employer's perspective there are three key areas of interest as we highlight below.

Approach to Consent

Much has been said about the reliance on consent to legitimise the processing of the personal data of employees. The Information Commissioner's Office's has expressed the view that it is not optimal for employers to seek to rely upon consent as it is difficult to establish that consent is "freely given" in the context of the employer/employee relationship. Employers have therefore been encouraged to move away from inserting blanket consent provisions in their employment contract, and ensuring they can satisfy one of the other conditions provided for the processing of ordinary or sensitive personal data.

The GDPR reinforces and strengthens this principle by placing an even higher threshold on consent. Consent under the GDPR (whether in respect of ordinary or personal data) is defined as "freely given, specific, informed and explicit" which in practice requires a statement or clear affirmation. It cannot be relied upon where there is a significant imbalance between the position of the data subject and controller. Where a consent provision appears in some broader document, it must be highlighted clearly and the individual should be informed of their right to withdraw their consent.

In light of these stricter requirements for securing consent, employers would be well-advised to update their template employment contracts to remove standard consent clauses, and otherwise to ensure their processing of employee data satisfies one of the other relevant conditions. Employee privacy notices will also need to be reviewed to ensure that all relevant information about the employer's data processing is covered.

Data Subject Access

The rules on data subject access are changing. The timescale for an organisation to respond will be reduced from 40 days to just one month, although this may be extended where necessary to take account of the complexity of the request. The £10 fee has also been abolished and employers will not be able to charge a fee in the majority of cases. According to the Ministry of Justice's Impact Assessment, the removal of the fee will increase the number of subject access requests by 25% to 40%, including those that are vexatious or frivolous.

The GDPR contains no guidance for employers tackling extensive subject access requests that require significant retrieval exercises, or dealing with requests made to fuel parallel litigation. Responding to these requests is still likely to be expensive and time-consuming, with the penalties for non-compliance increasing. Employers can take limited comfort in the fact that where requests can be said to be "manifestly excessive", particularly in terms of their repetitive nature, a reasonable fee can be charged or the employer may refuse to act on the request at all. What will amount to "manifestly excessive" remains to be seen, but the exception is going to be narrow and it will be the employer's burden to demonstrate why the request is manifestly excessive. All in all, this is unwelcome news for those employers who face regular subject access requests from employees and ex-employees in the context of some parallel dispute.

Appointment of Data Protection Officer

Under the GDPR there is a new mandatory requirement for certain organisations to appoint an in-house Data Protection Officer. Subject to any last minute changes to the text of the GDPR, this requirement will apply to public bodies and organisations whose core activities involve large scale processing of sensitive personal data, or regular and systematic

monitoring of personal data on a large scale. The majority of large organisations will therefore be caught by this provision.

The DPO will be tasked with giving advice on compliance, monitoring policies and audits, ensuring documentation

requirements are followed and co-operating with the applicable supervisory authority. The DPO will have a hybrid, self-regulating role within the organisation. He/she must be independent and cannot be instructed on how to carry out their tasks. He/she must also report to the highest level of management. In addition, the DPO will have special "protected status" as they cannot be dismissed or penalised for performing their tasks; such protection is novel for UK employers, and goes beyond existing protection available to "whistleblowers". This in turn may create challenges for an employer where there is a genuine need to take action against a DPO, for example, to address legitimate performance concerns.

According to a study commissioned by the ICO into the implications of the GDPR, the vast majority of companies with over 250 employees already employ staff with a job role focused on data protection compliance. In these cases, except for making the necessary changes to the job specification, the organisation should not need to expend significant resources to comply with new requirements. Other organisations will need to recruit to this position, and a DPO position may well command a significant remuneration package to reflect their importance and seniority.

Actions to be taken now

- Implement a clear protocol to reduce the burden of responding to subject access requests (particularly for organisations who regularly receive requests);
- Consider appointing a Data Protection Officer or update existing job descriptions;
- Analyse the legal basis for the processing of personal data that does not involve consent. Employers would be well advised to abandon their standard consent clauses, and instead audit their data processing to confirm other processing conditions apply;
- Employee privacy notices will also need to be updated to cover the information prescribed by the GDPR;
- Train and educate staff on data protection responsibilities.

We are expecting guidance from the ICO in due course to assist employers to address their revised responsibilities when processing employee personal data.

Follow us on twitter @DACBprivacy

UK Developments

Click the below headings to read more...

- ICO publishes revised privacy notices code of practice for consultation
- Committee, police and HMRC give view on investigatory powers proposal
- ICO publish small business guide to IT security
- Google confirm right to be forgotten should be applied to all searches made from within the EEA
- ICO publishes interim guidance on cross-border data transfers
- EDPS publish 'Umbrella Agreement' opinion
- House of Commons Committee releases report on the 'Big Data Dilemma'
- ICO produce Wi-Fi analytics guidance
- ICO blogs on stopping and identifying nuisance call companies
- Surveillance Camera Commissioner publishes self assessment tool and certification scheme
- European Economic and Social Committee release view on EC's digital strategy
- ICO publish rights for the future 3 year plan
- EU-US Privacy Shield update
- ICO undertakings
- ICO enforcement notices
- ICO monetary penalties

EU Data Protection Regulation Developments

Click the below headings to read more...

- GDPR update
- WP29 release action plan concerning the implementation of the GDPR
- UK confirms that it will not opt-in to Article 43a of the GDPR

Updates From Across The World

Click the below headings to read more...

Key Dates Calendar

Key date	Issue	Action
24 March 2016	ICO consultation to revise the Privacy Notices Code	Organisations should consider reviewing the ICO's Privacy Code proposals and delivering to the ICO any feedback that it may have. If organisations wish to respond on the consultation, they should do so by 24 March 2016. The consultation document can be accessed here.

Glossary

Please click here for the Glossary.

Authors

Khurram Shamsee
London - Walbrook
kshamsee@dacbeachcroft.com

Rhiannon Webster
London - Walbrook
rwebster@dacbeachcroft.com

DAC BEACHCROFT