Taking action: enforcement of data protection by design and by default

Peter Given, Legal Director, and Amy Eames, Associate, with Womble Bond Dickinson (UK) LLP, explore two real-life case studies demonstrating the importance of including data protection by design and by default into projects involving the processing of personal data

Peter Given is leading a half-day Workshop on 'Data Protection by Design and by Default - What's Actually Required' at the 18th Annual Data Protection Practical Compliance Conference taking place in London on 10th and 11th October. See the website for details www.pdpconferences.com

Prior to the General Data Protection Regulation 2016/679 ('GDPR') taking effect, 'privacy by design' was seen simply as good practice by the UK's Information Commissioner's Office ('ICO'). Now under the GDPR, data protection by design and by default is a legal requirement. Failure to comply with this requirement can be punished by administrative fines of up to €10 million or 2% of annual worldwide turnover in the preceding financial year (whichever is highest).

As this is not a new concept, previous enforcement actions taken by the ICO can shed light on how the regulator has in the past enforced data protection by design and by default and how it may approach this in the future. In this article, we look at two case studies below involving Google DeepMind and the Metropolitan Police Service. These enforcement actions show the importance of including data protection by design and by default in the design, operation and management of any project that involves the processing of personal data, and the consequences if you do not.

What is data protection by design and by default?

Data protection by design requires organisations to build the Data Protection Principles (including as set out in Article 5 of the GDPR) into the design, operation and management of any project that involves the processing of personal data. The requirements are set out more specifically in Article 25(1) of the GDPR, which states that a controller shall 'implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the Regulation and to protect the rights of data subjects.'

Data protection by design will need to be implemented during the 'design' phase before the processing starts and during the lifecycle of the processing. In doing so, the controller will need to consider the state of the art and costs of implementation, as well as the risks to the rights and freedoms of the individual, and the nature, scope, context and purpose of the processing.

Data protection by design also influences a controller's choice of processor. Controllers are required to only use processors which provide 'sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject', under Article 28(1) of the GDPR. Therefore, it is important for controllers to choose processors who will help them comply with their data protection by design obligations.

Data protection by default is the requirement to implement appropriate technical and organisational measures to ensure that, by default, only those personal data which are necessary for each specific purpose are processed. The requirements are set out more specifically in Article 25(2) of the GDPR which state that data protection by default applies to:

- the amount of personal data collected (the data minimisation principle);
- the extent of their processing (the purpose limitation principle);
- the period of storage (the storage limitation principle); and
- the accessibility of the personal data (the integrity and confidentiality principle).

The seven foundational principles of privacy by design published prior to the GDPR by the Information and Privacy Commissioner of Ontario, and referred to in the ICO's guidance on data protection by design and by default (copy at www.pdpjournals.com/docs/887991) can assist. These seven principles acknowledge that whilst "privacy by design is not necessarily equivalent to data protection by design, these foundational principles can nevertheless underpin any approach you take", and that "one means of putting these concepts into practice is to develop a set of practical, actionable guidelines that you can use in your organisation, framed by your assessment of the risks posed and the measures available to you."

Other practical examples of data protection by design and by default include:

- ensuring the minimum level of personal data are being collected for the purpose(s) of collection;
- carrying out a data protection impact assessment for high risk processing activities. The ICO states in its guidance on data protection by design and by default that data protection impact assessments are "an integral part of data protection by design and by default";
- implementing data protection and information security training for staff and creating a work culture which is privacy aware and takes privacy seriously; and
- implementing data protection and information security policies and procedures in order to help meet the Data Protection Principles (e.g. procedures for when onboarding processors and for the sharing of personal data with other third parties).

> ***"Data protection by design requires organisations to build the Data Protection Principles (including as set out in Article 5 of the GDPR) into the design, operation and management of any project that involves the processing of personal data."***

Being able to demonstrate compliance with data protection by design and by default is essential. The implementation of both will vary from organisation to organisation and project to project, which allows controllers flexibility as to how they implement these concepts at the 'design' phase and during the lifecycle of the processing.

Becoming certified may assist. Indeed, Article 25(3) of the GDPR allows a controller to help demonstrate its compliance with data protection by design and by default by complying with an approved certification mechanism. Whilst no approved certification mechanisms are currently in place in the UK, the European Data Protection Board has recently adopted its guidelines on certification and the accreditation of certification bodies under the GDPR. Therefore this is an area which in the future may help a controller continue to show they are complying with their data protection by design and by default requirements.

Lessons to be learnt from previous enforcement actions

1. Carry out a data protection impact assessment first (where required). In 2017, the ICO investigated the Royal Free London NHS Foundation Trust (Trust) and the sharing of approximately 1.6 million patient details with DeepMind Technologies Limited (DeepMind), for the purpose of developing a new mobile app for the diagnosis and detection of acute kidney injury. DeepMind was said to be acting as a processor on behalf of the Trust (as controller) in relation to this purpose. Findings from the ICO investigation revealed that:

- the Trust had carried out a privacy impact assessment; however, the assessment had been carried out after the personal data were shared, rather than during the design phase. The ICO was concerned that a full privacy impact assessment had not been carried out before the project was started, given the large amount of sensitive data being shared. The ICO expected that such an assessment would be carried out first during the design phase;
- the ICO was not convinced by the explanation given by the Trust that DeepMind needed all the personal data shared. This demonstrates that the personal data being processed must be limited to what is necessary for the purpose(s) of the processing;
- the agreement with DeepMind did not ensure that DeepMind only had access to the minimum level of personal data needed for the development of the new mobile app (i.e data protection by default) or an obligation on DeepMind only to use the personal data for this purpose. This demonstrates that the ICO expects more robust agreements in place with third parties who receive personal data with appropriate restrictions and obligations to protect the personal data;
- the ICO also advised the Trust to (i) review any 'bring your own device' issues, as personal data could be reviewed on devices used by clinicians; (ii) ensure access audit trails and restrictions on access were in place; and (iii) ensure personal data are deleted in accordance with the stated retention period. This reiterates that the Data Protection Principles (including as set out in Article 5 of the GDPR) need to be taken into account throughout the lifecycle of the processing — from start to finish.

Following the investigation, the Trust was asked to give an undertaking to re-do its privacy impact assessment within two months and to audit the data processing arrangements with DeepMind within three months. The Trust then had to report back to the ICO.

2. Build the data protection principles into the design, operation and management of any project that involves the processing of personal data. The next highlighted enforcement action demonstrates the importance of building privacy by design and by default into projects involving the processing of personal data at the design phase. The Metropolitan Police Service ('MPS') created a Gangs Matrix database to track potential criminal activities of alleged gang members, which was compiled

(Continued on page 12)

(Continued from page 11)

of data from 32 London boroughs. In 2018, the ICO investigated the operation of this database and how the local boroughs were using the personal data, and found serious data protection breaches. These included excessive processing and sharing of personal data with third parties, concerns as to the accuracy and retention of the personal data, data being transferred in a non-secure manner and no governance, oversight or audit of the processing or data sharing agreements in place.

Findings from the ICO's investigation revealed that the lack of guidance on the requirements of data protection law and practice by the MPS, and ensuring that such guidance was being followed, were both contributing factors to how the local boroughs were using the personal data. The ICO stated in its enforcement notice that "had a through and detailed privacy/data protection impact assessment on the Gangs Matrix been carried out at any time during the operation of the Model, such failings should have been identified and corrected".

The ICO issued the MPS with an enforcement notice requiring the MPS to ensure the database comprised with data protection laws within the short time period of six months, including but not limited to carrying out a data protection impact assessment, deleting any personal data no longer needed and implementing a retention schedule, implementing staff training and policies for using the personal data and for performing audits, improving security and access restrictions, and carrying out a full review of the data sharing arrangements in place for compliance with data protection laws. The MPS was also required to report its progress on a monthly basis to the ICO.

Conclusion

The above enforcement actions show the importance the ICO places on data protection by design and by default. Whilst these cases occurred prior to the GDPR, the ICO is likely to continue to focus on ensuring data protection by design and by default is embedded within the design, operation and management of any project that involves the processing of personal data. We can expect more detailed guidance on this area to follow from the ICO, which appears likely to be published after the regulator has finished its consultation on age appropriate design. The European Data Protection Board also stated in its Work Program for 2019/2020 that it plans to issue guidelines on data protection by design and by default.

To learn more about data protection by design and by default in a practical context, including understanding what may need to be changed in your organisation, designing an effective framework so that data protection by design and by default are built in and creating necessary awareness amongst staff member, we invite you to register for our Workshop on day 2 of PDP's 18th Annual Data Protection Compliance Conference. See www.pdpconferences.com for further details.

Peter Given and Amy Eames
Womble Bond Dickinson (UK) LLP
peter.given@wbd-uk.com
amy.eames@wbd-uk.com