A&L Goodbody

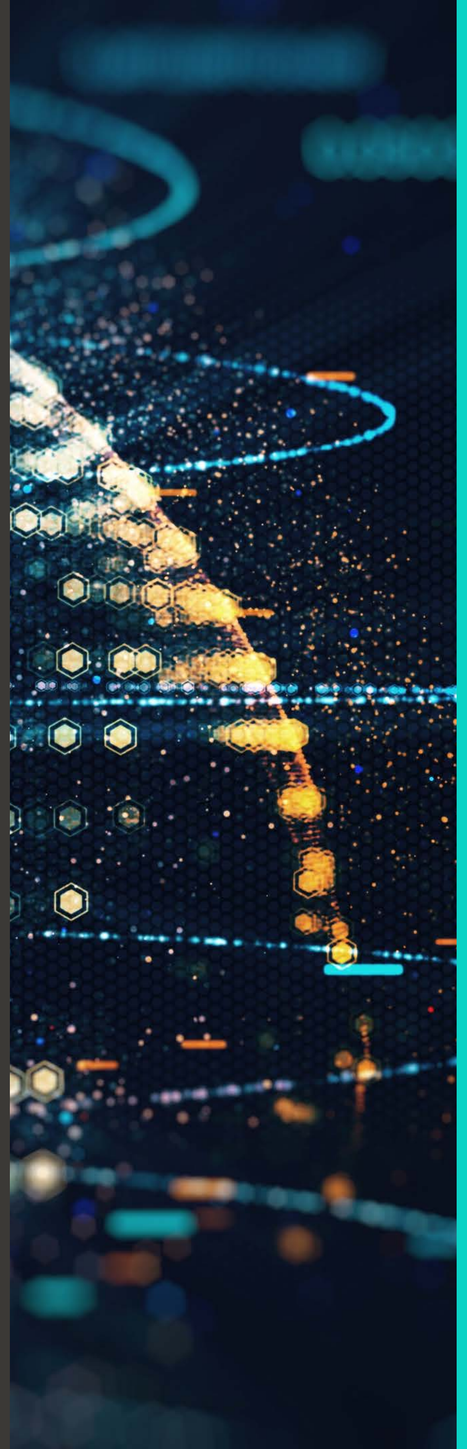
COMMERCIAL TECHNOLOGY

WhatsApp decision considers scope of transparency obligations under the GDPR

The DPC recently fined WhatsApp €225 million for failing to discharge its transparency obligations under the GDPR. The decision will have implications for all businesses, particularly regarding their privacy notices and transparency obligations.

The decision sets out the DPC's high expectations in regard to businesses' transparency obligations. It also clarifies the relevance of the consolidated turnover of the entire group of companies when calculating both the maximum fining cap, and the appropriate fine to impose.

5 MIN READ



Earlier this month, the Irish Data Protection Commission (**DPC**) published its decision in respect of its statutory inquiry into WhatsApp Ireland Ltd (**WhatsApp**). The DPC imposed a €225m fine on WhatsApp for failure to comply with its transparency obligations under Articles 5(1)(a), and 12-14 of the GDPR.

This is the highest fine ever issued by the DPC and the second highest by any EU regulator to date (the highest being the €746m fine imposed by the Luxembourg authority on Amazon). The DPC also issued a reprimand, and ordered WhatsApp to bring its processing operations into compliance by taking a range of specified remedial actions within a period of 3 months.

Why is this case important?

The 266-page decision clearly sets out the DPC's expectations in relation to the information that businesses must provide to individuals when collecting their personal data, in order to comply with their transparency obligations under Articles 5(1)(a) and 12-14 of the GDPR. The DPC forensically examined WhatsApp's privacy policy against the information prescribed by the GDPR, and found no margin of discretion for WhatsApp to interpret their obligations in a pragmatic manner. On the contrary, the DPC expects a high degree of granularity in the information that must be provided to individuals, irrespective of information fatigue.

In light of the DPC's strict interpretation of the information requirements and the manner in which it should be delivered under Articles 12-14, it is important that businesses take time to review and, where necessary, update their Privacy Notices to ensure they comply with their transparency obligations.

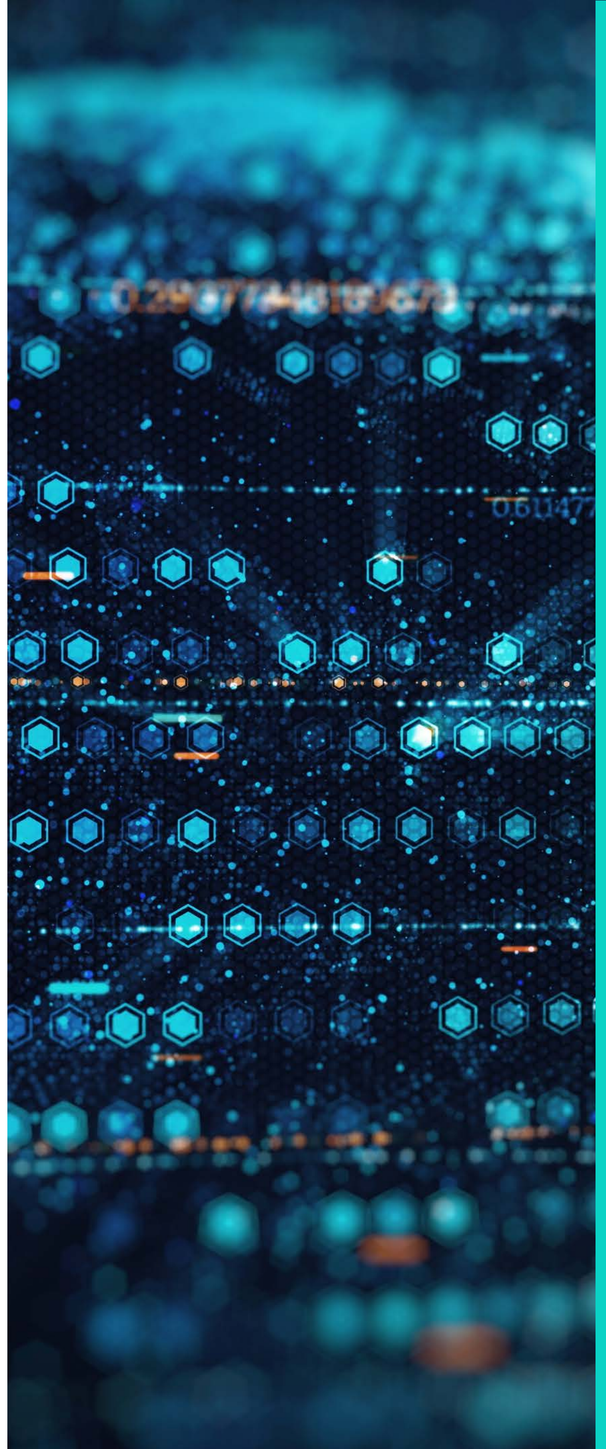
The decision also provides further clarity regarding the scope of the concept of "*personal data*" under the GDPR, and the high threshold that must be reached before personal data will be deemed to be anonymised and fall outside the remit of the GDPR. In addition, it clarifies that an undertaking's turnover is relevant for the purposes of calculating the appropriate administrative fine under the GDPR to ensure it is "*effective, proportionate, and persuasive*", as well as for determining the maximum fine that can be imposed.

Background

On 10 December 2018, the DPC commenced an own-volition inquiry pursuant to section 110 of the Data Protection Act 2018, following complaints from users and non-users about WhatsApp's processing activities. The inquiry focussed on examining whether WhatsApp had discharged its transparency obligations under Articles 12-14 GDPR with regard to the provision of information to both users and non-users of WhatsApp's service. This included transparency in the context of data sharing between WhatsApp and other Facebook companies.

In December 2020, following a lengthy investigation, the DPC (acting as Lead Supervisory Authority) submitted a draft decision to all Concerned Supervisory Authorities (**CSAs**) for their opinion, as required by Article 60 of the GDPR. The DPC was unable to reach a consensus with the CSAs on objections raised, and therefore triggered the dispute resolution process under Article 65 of the GDPR. Multiple objections were raised by the CSAs, including whether a mobile phone number of a non-user was personal data after it had been subjected to a lossy hashing procedure; possible additional infringements of the GDPR; whether the DPC had correctly interpreted Article 83(3) in finding that, in a case of the same or linked processing operations, a fine could only be imposed in respect of the most serious infringement rather than an accumulation of fines for each infringement finding; and the appropriate method for calculating turnover.

On 28 July 2021, the European Data Protection Board (**EDPB**) adopted a binding decision, which included a clear instruction requiring the DPC to reassess and increase its proposed fine (€30m - €50m) on the basis of a number of factors. Following this reassessment, the DPC imposed an administrative fine of €225m on WhatsApp.



The DPC Decision

The DPC's decision is divided into five parts. We have examined the DPC's findings in respect of each part below:

1. Transparency in the context of non-users of WhatsApp
2. Transparency in the context of users of WhatsApp
3. Transparency in the context of sharing of personal data between WhatsApp and other Facebook group companies
4. Compliance with the Transparency principle
5. Calculation of the administration fine

Part 1: Transparency in the context of non-users

(i) Does a non-user's mobile phone number constitute 'Personal Data' under the GDPR?

WhatsApp offers an optional 'Contact Feature' feature which allows users to request WhatsApp to access the phone numbers in their address book for the purpose of determining which of their contacts are WhatsApp users. The question therefore arose as to whether in accessing those phone numbers WhatsApp was processing non-users' personal data, and therefore had an obligation under Article 14 of the GDPR to provide transparency information to non-users about such processing.

The DPC determined that, prior to various hashing techniques being deployed by WhatsApp, the mobile phone number of a non-user constitutes personal data, on the basis that an individual is "*identifiable*" from his/her mobile phone number. Personal data is defined in Article 4(1) GDPR as "*any information relating to an identified or identifiable natural person*". In determining whether a person is identifiable, Recital 26 of the GDPR requires an assessment of "*all of the means reasonably likely to be used*" by the controller or a third party to identify the natural person directly or indirectly, taking into account objective factors such as the costs, the amount of time required for identification, and available technology.

The DPC stated that Recital 26 does not require an assessment of the likelihood of whether or not the controller or a third party might want or need to avail of those means. The phone numbers constitute personal data under the GDPR, on the basis that there are means available that are "*reasonably likely to be used*" in the event that WhatsApp or a third party forms the intention to identify the owner of the number. Accordingly, it did not matter that WhatsApp had no desire to identify the owners of the mobile phone numbers. The DPC stated that the decision of the Court of Justice of the European Union (**CJEU**) in the *Breyer* case supports this approach.

(ii) Does a non-user's hashed mobile phone number constitute personal data?

The DPC, in its draft decision, concluded that the hashed phone numbers of non-users did not constitute personal data. This was due to the fact that the phone number is irretrievably deleted after the hashing process, and the lossy hash generated can represent any of at least 16 mobile phone numbers.

However, in its Article 65 decision, the EDPB directed the DPC to find that the mobile phone numbers of non-users constitute personal data following the hashing process. The EDPB considered that given the technical means and data available to WhatsApp, its capacity to single out data subjects is too high to consider the dataset anonymous after the hashing process. It considered the hashing process effectively pseudonymised rather than anonymised the phone numbers, and therefore they constituted personal data.

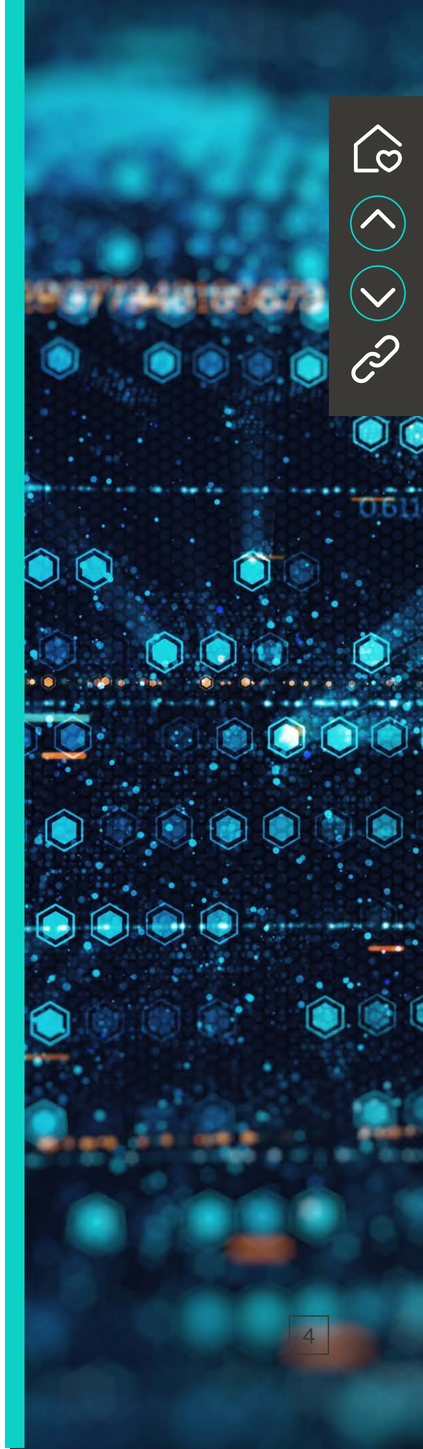
(iii) Is WhatsApp a Controller or Processor when processing non-user data?

The DPC found that when processing non-user personal data, WhatsApp does so as a data controller, and not as a processor, as only WhatsApp makes all the decisions in respect of the core aspects of the processing of non-user data.

(iv) Did WhatsApp comply with its transparency obligations towards non-users under Article 14 of the GDPR?

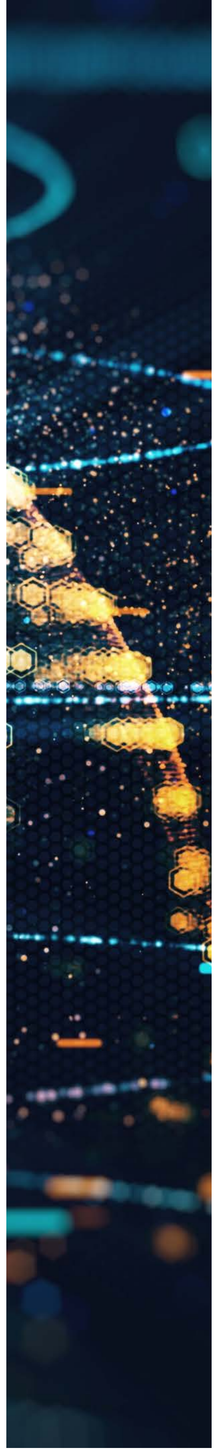
In acting as a controller of non-user personal data, the DPC found that WhatsApp had failed to comply with its obligations to non-users pursuant to Article 14 of the GDPR.

The DPC also noted that even if WhatsApp were to rely on the exception to the transparency information requirements, set out in Article 14(5)(b) GDPR (namely that the provision of such information would involve a disproportionate effort), WhatsApp would still be required to take measures to make the information publicly available.



(v) Were the DPC's findings consistent with the EU law principle of proportionality?

WhatsApp argued that the DPC's findings in relation to its transparency obligation to non-users was inconsistent with the principle of proportionality. In response, the DPC stated that the non-user data undergoing processing by WhatsApp is very limited, as are the processing operations that are applied to the data concerned. Accordingly, the preparation of the required information should not be burdensome for WhatsApp.



Part 2: Transparency in the context of users

The DPC also considered the extent to which WhatsApp discharged its transparency obligations under Articles 13 and 12(1) GDPR to users of its service. Whilst Article 13 GDPR sets out a list of prescribed information that must be communicated to users, Article 12 GDPR addresses the manner in which this information must be communicated, and affords the controller discretion, in terms of the formulation and method of delivery of the specified information. The DPC stated, however, that "this is a very limited discretion…given the express requirement for the information to be provided in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child*'."

(i) Compliance with Article 13(1)(a) - the identity and contact details of the controller

WhatsApp had complied with its obligations under Article 13(1)(a). WhatsApp Ireland Limited is clearly identified as the relevant controller at the outset of the privacy policy, and the "*Contact Information*" section of the Policy contains a link for users to contact WhatsApp,

(ii) Compliance with Article 13(1)(b) - the contact details of the Data Protection Officer (where applicable)

WhatsApp had complied with its obligation under Article 13(1)(b). The "*Contact Information*" section includes a link which generates an email to their Data Protection Officer. The information again is in a location that the user might expect to find this information.

(iii) Compliance with Article 13(1)(c) – the purposes and legal basis for processing

WhatsApp had failed to comply with its obligations pursuant to Article 13(1)(c) and Article 12(1) which requires the controller to provide meaningful information enabling the data subject to understand: (i) which personal data are processed; (ii) for what processing operation; (iii) the purpose of the processing and (iv) legal basis for the processing. Such information must be presented in a way that clearly links each of these elements.

The DPC rejected WhatsApp's claim that its proposed approach was inconsistent with the EU law principle of proportionality, and that Article 13(1)(c) explicitly requires only the purpose and legal basis for the processing to be identified.

In concluding that WhatsApp had failed to comply with its obligations under Article 13(1)(c), the DPC examined the information that WhatsApp provided in respect of each legal basis it relied on for processing personal data. It is worth noting that in regard to WhatsApp's reliance on the 'compliance with a legal obligation' basis under Article 6(1)(c), the DPC found that where a controller intends to ground a processing operation on 'compliance with a legal obligation', it should identify the EU or Member State law giving rise to the obligation. Similarly, if relying on the 'public interests' legal basis under Article 6(1)(e), the DPC said a controller must identify the EU or Member State law giving rise to the obligation to process the data.

WhatsApp submitted that it cannot have been the legislative intention to require a controller to exhaustively list all legal obligations that it is subject to in order to comply with its obligation under Article 13(1)(c) GDPR, and such an approach is simply not feasible for controllers. The DPC disagreed, stating: "*A controller either processes personal data pursuant to a requirement set out in EU or Member State law or it does not. If it does, then all that is required is for the controller to inform the data subjects concerned about that processing along with the underlying legal requirement*".

(iv) Compliance with Article 13(1)(d) - legitimate interests pursued by the controller or third party (where applicable)

In its draft decision, the DPC found that sufficient information had been provided, such that the user is enabled to understand the legitimate interests being pursued. The information has been provided by way of a series of bullet points, under several identified objectives. In this way, the DPC found that the user can clearly identify which legitimate interests are being pursued under each identified objective.

However the EDPB, in its binding decision, found that WhatsApp had not provided specific information about which legitimate interests relate to each processing operation, and which categories of personal data are being processed for which legitimate interest. The EDPB therefore instructed the DPC to find that WhatsApp had failed to comply with Article 13(1)(d).

(v) Compliance with Article 13(1)(e) - the recipients or categories of recipients of the data

The DPC found that the information provided did not enable the user to understand what categories of personal data will be sent to which category of recipient, nor the purpose of such transfers, and therefore the consequences for the user. In addition the DPC held that there were deficiencies in the manner in which information about recipients was provided, as it was scattered throughout the Terms of Service, Privacy Policy and other documents. Therefore WhatsApp had failed to comply with Article 13(1)(e) and 12(1).

(vi) Compliance with Article 13(1)(f) - international data transfers

The DPC held controllers are required to provide information such that data subjects are informed in a "*definitive*" manner whether or not an adequacy decision exists to support the transfer of specified categories of personal data, and enable the data subject to access more information about the adequacy decision(s) being relied on. WhatsApp's privacy policy was insufficient, as it provided that it "*may*" rely on an adequacy decision "*if applicable*".

In addition, the DPC found that providing links to the European Commission's website containing the adequacy decisions and information on the Standard Contractual Clauses was insufficient. The DPC noted that the EDPB Transparency Guidelines make it clear that the data subject should be able to access (or obtain access, if access is not directly provided) to the specific set of standard contractual clauses or specific adequacy decision being relied on. Accordingly WhatsApp was found to have infringed Article 13(1)(f) and 12(1).

(vii) Compliance with Article 13(2)(a) – retention criteria/retention periods

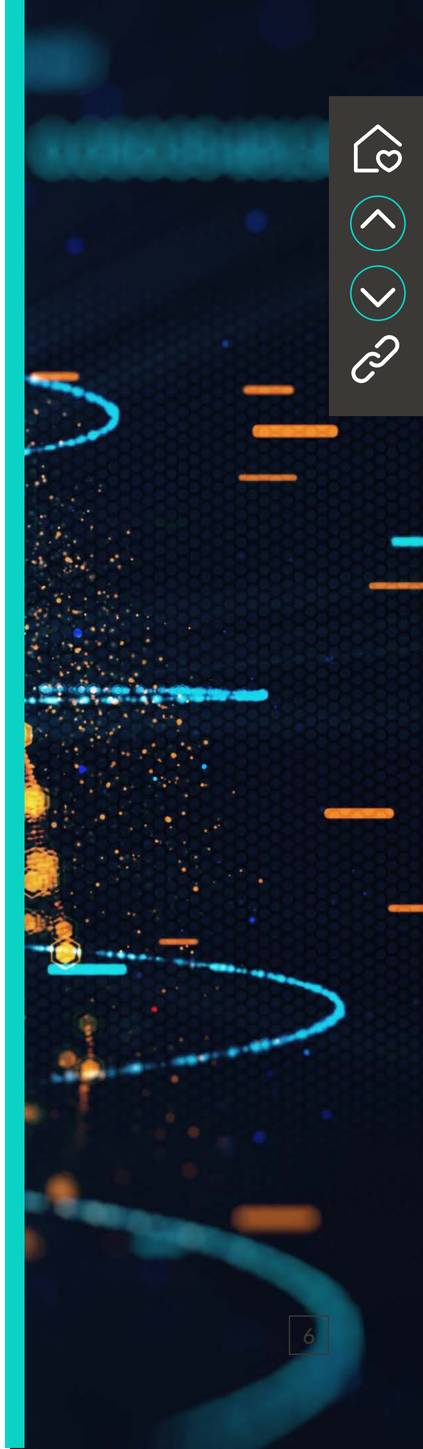
The DPC found that no meaningful information had been provided in relation to the criteria used to determine if, and for how long, a user's personal data is retained following the deletion of his/her account. Accordingly WhatsApp was found to have infringed Article 13(2)(a).

(viii) Compliance with Article 13(2)(b) – data subjects rights

The DPC held this information was provided in a clear and concise way, and was easy to locate in an appropriately named section of the policy entitled "*How to exercise your rights*".

(ix) Compliance with Article 13(2)(c) - the existence of the right to withdraw consent

The DPC found that the "*How to exercise your rights*" section does not include reference to the right to withdraw consent to processing or how a data subject can go about exercising this right. Given the title of this section, the DPC concluded that this is where the data subject is most likely to search for this information, and reference to the right to withdraw consent should be included there.



The DPC also found that WhatsApp had referenced the right to withdraw consent, but had omitted reference to the qualifier "*without affecting the lawfulness of processing based on consent before its withdrawal*".

Accordingly, WhatsApp had infringed Article 13(2)(c) and Article 12(1).

(x): Compliance with Article 13(2)(d) - right to lodge a complaint with the DPC

The DPC found that this information was provided in a clear and concise way, albeit in a confusing place – namely the "*Contact Information*" section of the policy. The DPC stated that this information should have been included or at least cross-referenced in the "*How to Exercise Your Rights*" section of the privacy policy, given that this is likely the place where a data subject will first go to learn about his/her rights.

The DPC directed WhatsApp to include a reference as to the existence of this right in the "*How to exercise your rights*" section of the policy.

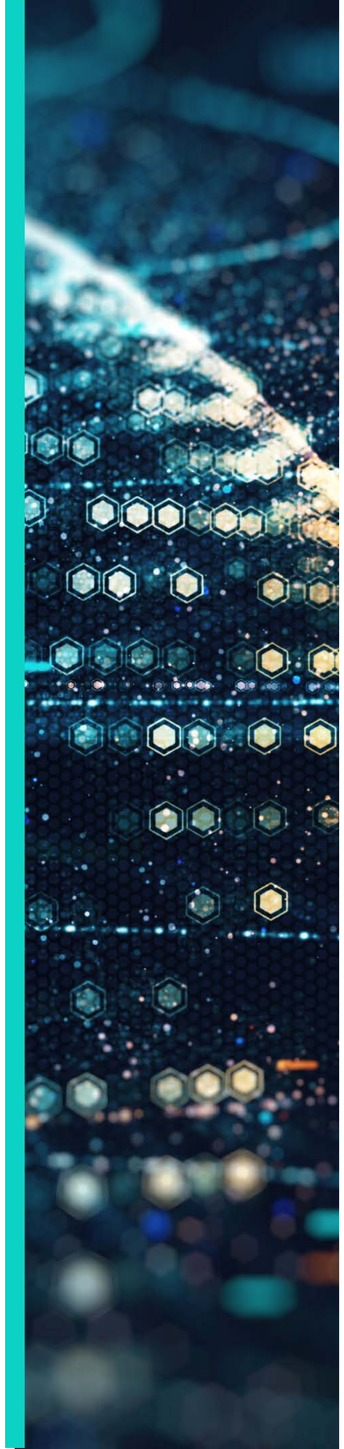
(xi) Article 13(2)(e) - whether the provision of the personal data is a statutory or contractual requirement, or a requirement to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data

The DPC noted that it stands to reason that WhatsApp need to process a certain minimum amount of personal data to provide their Service, but the extent of the minimum personal data required is not clear from WhatsApp's privacy policy. Further, the (possible) consequences of failure to provide data are not clearly set out for the data subject.

The DPC (following a direction by the EDPB in its binding decision to do so) found that WhatsApp had failed to comply with its obligation under Article 13(2)(e).

(xii) Article 13(2)(f) - the existence of automated decision-making, including profiling (if applicable)

As WhatsApp does not engage in any such automated decision-making, there is no obligation to provide this information.



Part 3: Transparency in the context of sharing users' personal data between WhatsApp and the Facebook Companies

The DPC found that WhatsApp had failed to comply with its transparency obligations pursuant to Articles 13(1)(c)-(e) and 12(1) in relation to how it shares personal data with the Facebook companies. The information provided about the sharing of data between WhatsApp and Facebook companies is spread over a number of different texts, and the DPC stated it would be unfair to expect a user to search the entire WhatsApp website to determine how their data were being shared with other Facebook companies, having failed to find sufficient information in the privacy policy itself. In addition, a significant amount of the information was so high level that it was meaningless.

The DPC held that unless WhatsApp has a concrete plan in place, that includes a definitive and imminent commencement date, to commence the sharing of personal data on a controller to controller basis with the Facebook companies for safety and security purposes, the misleading legal basis notice and Facebook FAQs should be deleted to reflect the true position.

Part 4: Article 5(1)(a) – Compliance the Transparency principle

The EDPB directed the DPC to amend her decision to include an infringement of the general principle of transparency set out in Article 5(1)(a) of the GDPR, as the Article 12-14 infringements reflect a "*significant level of non-compliance*" which impacts on all of the processing carried out by WhatsApp.

The EDPB noted that WhatsApp's cumulative breaches of Articles 12-14 resulted in it failing to provide over 41% of the information required under Article 13 GDPR to relevant users, and there had been a total failure to provide non-users with the required information.

Part 5: Exercise of Corrective Powers

Part 5 of the DPC's decision concerns its calculation of the administrative fine. Having regard to the criteria in Article 83(2), the DPC decided that an administrative fine was warranted, as all four infringements of Articles 5(1)(a), 12, 13, and 14 GDPR were very serious in nature, and gravity, and go to the heart of the principle of transparency. The DPC characterised all of the infringements as negligent, and the infringement of Article 14 as demonstrating "*a high degree of negligence*", which was taken into account as an aggravating factor.

Mitigating Factors

The only mitigating factors, in the DPC's view, were the limited categories of personal data undergoing processing, in particular in regard to non-users, and also WhatsApp's willingness to amend its privacy policy and related material. However, the DPC said she was unable to attribute significant weight to either of these factors, given the overall seriousness and severity of the infringements and in light of the fact that as of December 2020, WhatsApp has only begun to implement changes to its privacy policy and related material.

EDPB Direction – Higher fine required

The EDPB instructed the DPC to impose a higher fine to reflect a number of conclusions reached by the EDPB, including:

- The relevant turnover for the purposes of calculating the fining cap under the GDPR is the "*global annual turnover of all the component companies of the single undertaking*". Accordingly, the EDPB concluded that the DPC should amend its draft decision in order to take into account the consolidated turnover of the entire Facebook Inc. group of companies.
- The relevant turnover is the one corresponding to the financial year preceding the date of the final (not draft) decision taken by the Lead Supervisory Authority pursuant to Article 65(6) of the GDPR.
- The turnover is relevant for the determination of the maximum fining cap, and for the calculation of the appropriate fine to ensure it is "*effective, proportionate and dissuasive*". The DPC, in its draft decision, had rejected the notion that the fine needs to have a noticeable impact on the profits of an undertaking.
- The amount of the fine shall appropriately reflect the aggravating factors identified in the draft decision under Article 83(2) GDPR (such as the number of affected data subjects), to ensure the fine is proportionate.
- The identified additional infringements of Articles 5(1)(a), 13(1)(d), 13(2)(e) and the extended scope of Article 14 GDPR are to be reflected in the amount of the fine, as brought up by several CSAs in their objections.
- All of the infringements are to be taken into account when calculating the amount of the fine, in accordance with the EDPB's interpretation of Article 83(3) GDPR. The fine that is imposed should not, however, exceed the total fine that can be imposed for the gravest infringement (which in this case was an infringement of Article 14).

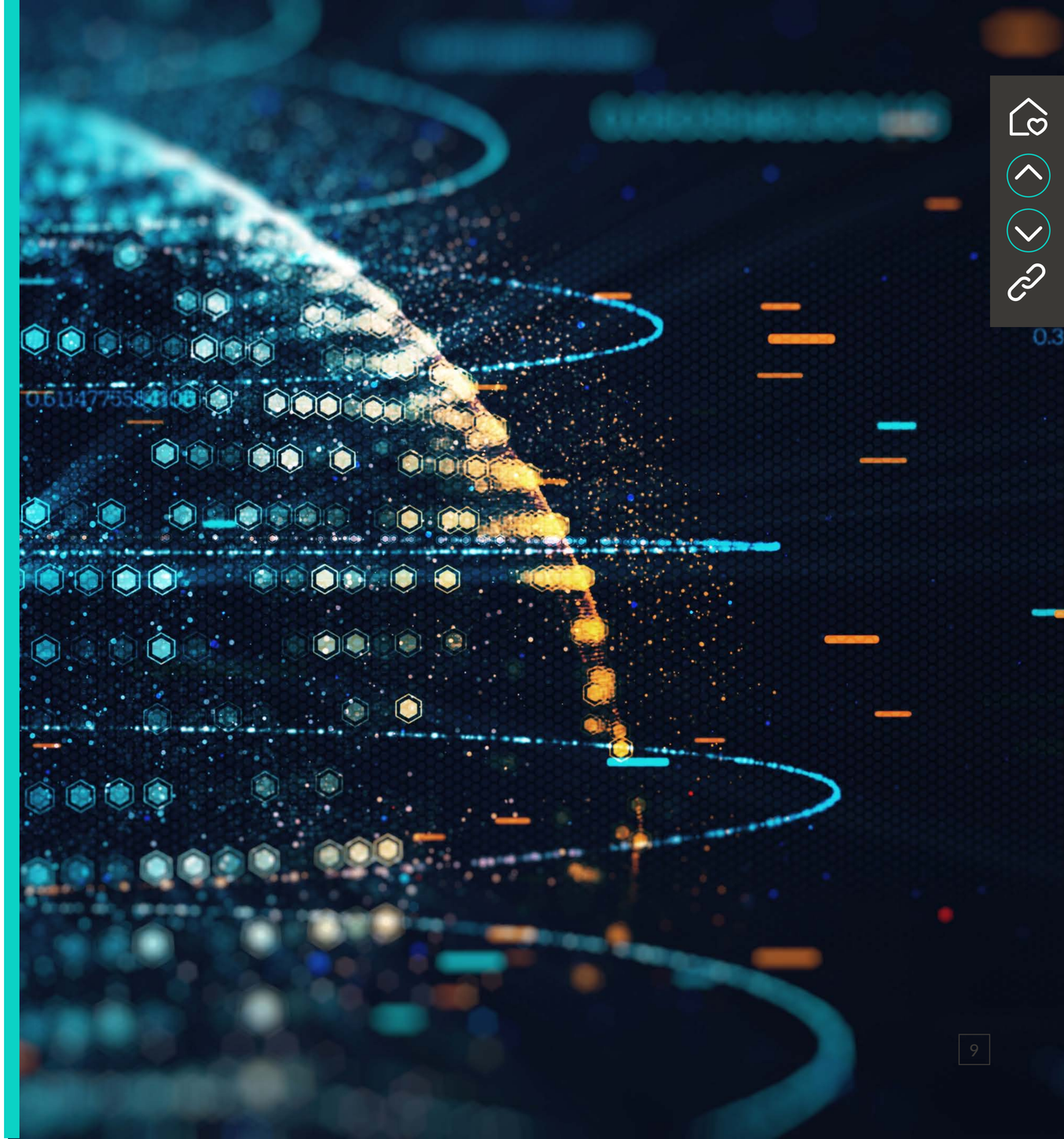
What happens next?

On 16 September 2021, WhatsApp issued judicial review proceedings against the DPC seeking an order quashing the €225m fine. In addition, WhatsApp has reportedly lodged a statutory appeal before the Irish courts against the DPC's decision, and further intends to bring an annulment action against the EDPB's decision to the CJEU.

Pending this appeal, it would be prudent for businesses to consider the expectations of the DPC set out in this decision, and review and update their Privacy Notices (where necessary) to ensure they comply with the transparency obligations under Articles 5(1)(a) and 12-14 of the GDPR. The decision highlights, in particular, the importance of providing clear and granular information to data subjects, to enable them to understand what categories of personal data are processed for which processing operation(s) and its purpose(s) and legal basis.

Businesses should also consider the manner in which the prescribed information is presented to data subjects. To ensure compliance with Article 12(1), the information should be easily accessible, presented separately to other non-privacy related information, and located in a place where the data subject would expect to find it. The DPC has warned that a data subject should not have to work hard to access the prescribed information nor be left wondering if he/she has exhausted all available sources of information.

The level of the fine imposed in this case, and the relevance of turnover when calculating not only the maximum fining cap, but also the appropriate fine to impose to ensure it is "*effective, proportionate dissuasive*" will likely impact the level of fines imposed by regulators in the future for violations of the GDPR.



A&L Goodbody

Key contacts

Chris Bollard
Partner
+353 1 649 2328
cbollard@algoodbody.com

Andrew Sheridan
Partner
+353 1 649 2766
asheridan@algoodbody.com

John Whelan
Partner
+353 1 649 2234
jwhelan@algoodbody.com

John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com

Andrea Lawler
Partner
+353 1 649 2351
alawler@algoodbody.com

Davinia Brennan
Knowledge Lawyer
+353 1 649 2114
dbrennan@algoodbody.com

Resources

DPC final decision dated 20 August 2021 — READ MORE

EDPB decision under Article 65 GDPR dated 28 July 2021 — READ MORE

EDPB Transparency Guidelines 2016/679 — READ MORE