









Appendix A - Summary of Directions and Findings

| <i>Outcome</i> | <i>Summary of Outcome</i> | <i>Location within Decision</i> |
|---|---|---------------------------------|
| Part 1: Transparency in the context of non-users | | |
| Finding | Prior to lossy hashing, the phone number of a non-user constitutes the personal data of that non-user in circumstances where the non-user can be indirectly identified by reference to his/her phone number | Paragraph 105 |
| Finding | After lossy hashing the phone number of a non-user, constitutes the personal data of that non-user in circumstances where the non-user cannot be identified | Paragraph 110 |
| Finding | When processing non-user data, WhatsApp does so as a data controller, and not a processor. | Paragraph 154 |
| Finding | WhatsApp has failed to comply with its obligations to non-users pursuant to Article 14. | Paragraph 177 |
| Part 2: Transparency in the context of users | | |
| Finding | WhatsApp has complied, in full, with its obligations pursuant to Article 13(1)(a). | Paragraph 249 |
| Finding | WhatsApp has complied, in full, with its obligations pursuant to Article 13(1)(b). | Paragraph 256 |
| Finding | WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(c) and Article 12(1). | Paragraph 399 |
| Finding | WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(d). | Paragraph 416 |
| Finding | WhatsApp has failed to provide the information required by Article 13(1)(e) and Article 12(1). | Paragraph 434 |
| Finding | WhatsApp has failed to comply with its obligations under Article 13(1)(f) and Article 12(1). | Paragraph 457 |
| Finding | WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(a) | Paragraph 476 |
| Finding | WhatsApp has complied, in full, with its obligations to provide information pursuant to Article 13(2)(b). | Paragraph 482 |
| Finding | WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(c) and Article 12(1). | Paragraph 496 |
| Finding (incorporating a Direction) | WhatsApp has broadly complied with the obligation arising pursuant to Article 13(2)(d), subject to the direction that WhatsApp include reference to the existence of this right under the "How You Exercise Your Rights" section so as to ensure that the data subject is presented with the required information in a place where he/she might expect to find it. | Paragraph 503 |
| Finding | WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(e) | Paragraph 520 |

| | | |
|--|--|------------------------|
| Part 3: Transparency in the context of any sharing of personal data between WhatsApp and the Facebook Companies | | |
| Finding (incorporating a Direction) | WhatsApp has failed to comply with its transparency obligations pursuant to Articles 13(1)(c), 13(1)(d), 13(1)(e) and 12(1) in relation to how WhatsApp works with the Facebook Companies. WhatsApp has broadly complied with its obligations pursuant to Article 13(1)(d). 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 elements of the Legal Basis Notice and Facebook FAQ should be deleted to reflect the true position. | Paragraphs 591 and 592 |
| Part 4: Article 5(1)(a) - Extent of compliance with the principle of Transparency | | |
| Finding | WhatsApp has failed to comply with its obligations pursuant to Article 5(1)(a) | Paragraph 595 |

| | Data obtained directly from data subject | Data not obtained directly from data subject | This information is extracted from WP 29 Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) |
|---|---|--|---|
| When should information be provided? | At the time the data are obtained. | Within a reasonable period of having obtained the data | |
| What information must be supplied? | | | Guidance / Further Reference from Article 29 Working Party |
| Identity and contact details of the controller and where applicable, the controller's representative | ✓ Art 13.1(a) | ✓ Art 14.1(a) | This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address etc.) |
| Contact details of the data protection officer – Where Applicable | ✓ Art 13.1(b) | ✓ Art 14.1(b) | See WP29 Guidelines on Data Protection Officers WP243 rev.01, last revised & adopted on 5 April 2017 |
| Purpose of the processing and the legal basis relied upon for the processing | ✓ Art 13.1(c) | ✓ Art 14.1(c) | In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 or Article 9 must be specified. |
| <i>Where legitimate interests is the legal basis of the controller or third party, the legitimate interests pursued</i> | ✓ Art 13.1(d) | ✓ Art 14.2(b) | The specific interest in question must be identified for the benefit of the data subject . As a matter of best practice, the data controller should also provide the data subject with the information from the balancing test, which should have been carried out by the data controller to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data. This is essential for effective transparency where data subjects have doubts as to whether the balancing test has been carried out fairly or they wish to file a complaint with a supervisory authority. |
| Categories of personal data | ✗ | ✓ Art 14.1(d) | This information is required in an Article 14 scenario because the personal data has not been obtained from the data subject who therefore lacks an awareness of which categories of their personal data the data controller has obtained. |
| Any recipient or categories of recipients of the personal data | ✓ Art 13.1(e) | ✓ Art 14.1(e) | The term "recipient" is defined in Article 4.9 such that a recipient does not have to be a third party. Therefore, data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term "recipient" and information on such recipients should be provided in addition to information on third party recipients. The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients. |
| Details of transfers to third country and safeguards | ✓ Art 13.1(f) | ✓ Art 14.1(f) | The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. <ul style="list-style-type: none"> adequacy decision under Article 45 binding corporate rules under Article 47 standard data protection clauses under Article 46.2 Derogations and safeguards under Article 49 etc.) Should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principle of fairness , the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named. |

| | | | |
|---|--|--|--|
| Retention period or criteria used to determine the retention period |  Art 13.2(a) |  Art 14.2(a) | <p>This is linked to the data minimisation requirement in Article 5.1(c) and storage limitation requirement in Article 5.1(e).</p> <p>The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/ purposes.</p> <p>It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing.</p> <p>Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods.</p> |
| <p>The existence of each of data subject's rights to</p> <ul style="list-style-type: none"> • access; • rectification; • erasure; • restriction on processing; • objection to processing • and portability. |  Art 13.2(b) |  Art 14.2(c) | <p>This information should be specific to the processing scenario and include a summary of what the right involves and how the data subject can take steps to exercise it and any limitations on the right</p> <p>In particular, the right to object to processing must be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information.</p> <p><i>[This specifically applies to Article 21.4 & Recital 70 – Relating to Direct Marketing i.e. “That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information”.]</i></p> <p>In relation to the right to portability, see WP29 Guidelines on the right to data portability WP 242 rev.01.</p> |
| The right to withdraw consent at any time where processing is based on consent (or explicit consent) |  Art 13.2(c) |  Art 14.2(d) | <p>This information should include how consent may be withdrawn, taking into account that it should be as easy for a data subject to withdraw consent as to give it.</p> |
| The right to lodge a complaint with a supervisory authority |  Art 13.2(d) |  Art 14.2(e) | <p>This information should explain that, in accordance with Article 77, a data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or of an alleged infringement of the GDPR.</p> |
| Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data |  Art 13.2(e) |  | <p>For example in an employment context, it may be a contractual requirement to provide certain information to a current or prospective employer.</p> <p>Online forms should clearly identify which fields are “required”, which are not, and what will be the consequences of not filling in the required fields.</p> |
| The source the personal data originates from and whether it came from publicly accessible sources |  |  Art 14.2(f) | <p>The specific source of the data should be provided unless it is not possible to do so <i>(The lifting of the requirement to provide data subjects with information on the source of their personal data applies only where this is not possible because different pieces of personal data relating to the same data subject cannot be attributed to a particular source.)</i></p> <p>If the specific source is not named then information provided should include:</p> <ul style="list-style-type: none"> • the nature of the sources (i.e. publicly/ privately held sources) • and the types of organisation/industry/ sector. |
| The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences. |  Art 13.2(f) |  Art 14.2(g) | <p>See WP29 Guidelines on automated individual decision making and Profiling 2016/679, WP 251. and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.</p> |

| | | |
|---|------------------------------------|---|
| When should information be provided? | At the time the data are obtained. | <p>Within a reasonable period of having obtained the data (within one month)</p> <p>If the data are used to communicate with the individual, at the latest, when the first communication takes place: or if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.</p> |
|---|------------------------------------|---|

Exemptions Not required when derogations in article 14(5)(b) to (d) apply. E.g it would pose a disproportionate effort for archiving in the public interest.