Published on *Jisc community* (https://community-stg.jisc.ac.uk)

2017 - Article 29 guidelines on profiling and automated decision making

Summary

1. Jisc does not consider that the wording of Article 22 of the General Data Protection Regulation (GDPR) supports the Working Party's assertion that automated decisions are prohibited. We believe this interpretation creates a significant risk to the privacy of individuals, increased by the draft guidelines' lack of clarity over which decisions fall within this ban. The interpretation and legal uncertainty are likely to reverse two objectives of the GDPR: by increasing, rather than reducing, the over-use of consent and deterring, rather than facilitating, the beneficial uses of new technologies. We therefore urge the Working Party to return to its 2013 position – that Article 22 creates a right to have automated decisions reviewed, not a ban.

Discussion

1. Article 22(1) of the GDPR states "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". Like all legal commentators we are aware of, Jisc has interpreted this as meaning that an individual about whom such an automated decision was made would be able to insist, if they wished, on that decision being reviewed by a human. Thus Article 22 would have the same nature as the other Articles beginning "The data subject shall have the right…" such as the right to object in Article 21.
2. This interpretation is supported by the UK Information Commissioner's 2017 consultation on Profiling [1] and the Working Party's 2013 Advice Paper [2], both of which presume that automated decision-making will continue, subject to additional obligations on data controllers and additional rights for data subjects. Indeed the Working Party specifically states that "[d]ata subjects should also have the right to access, to modify or to delete the profile information attributed to them and to refuse any measure or decision based on it **or have any measure or decision reconsidered with the safeguard of human intervention**" [our emphasis].
3. We are therefore surprised to find the Working Party now coming to a very different interpretation [3]. Rather than a retrospective right to have decisions reviewed, page 9 of the draft guidelines [3] states that "as a rule, there is a prohibition on fully automated individual decision-making, including profiling that has a legal or similarly significant effect". Given the serious implications of this interpretation and the fact that it contradicts a long-standing and widespread legal view, we would have expected some discussion and analysis of how this new interpretation was reached. However the draft document provides none.
4. Under the Working Party's interpretation, automating many decisions will be illegal and subject to a fine of up to €20M. If such a regime is to be created, we consider it essential

that it is made perfectly clear to data controllers which automated decisions are banned and which permitted. Instead the draft guidelines set out a very wide range of possible decisions – from refusal to rent a bicycle to refusal to permit a house purchase – without saying whether any of these are, or are not, banned. This suggests that the dividing line may fall anywhere within this range of significance or, indeed, outside it. A data controller that wishes to be sure of compliance might well conclude that even decisions as inconsequential as cycle hire must be inspected by a human: a data controller that wished to test the boundaries of the law might equally well conclude that a decision as significant as refusing a home loan could be taken entirely algorithmically.

Examples of likely harm

1. We provide two examples, from our current activity, of the harm likely to result from the threat of massive fines combined with a complete lack of clarity of when they will apply. Both activities are highly beneficial to data subjects. In each case Jisc has documented and encouraged the use of the Article 6(1)(f) balancing test – which often favours automated processing over human inspection – to ensure the activities also protect individuals' privacy. Not only will the draft guidelines eliminate the potential benefits that the Working Party recognises in automated decision making, in many cases they will result in greater privacy intrusion and loss of data protection and other rights.
2. Many organisations and network operators have – in support of their obligations under GDPR Art.24(1) and Article 4(1) of the ePrivacy Directive – implemented automated network defence systems to protect their users, systems and data from malicious network traffic. Such systems aim to identify Internet Protocol (IP) and e-mail addresses associated with such traffic and to block them before they are able to cause harm. Automated systems can detect known patterns of hostile traffic and block them within seconds, rather than the hours it may take skilled humans to do so. Since both IP and e-mail addresses are considered personal data under the GDPR, this appears to constitute automated decision-making within the meaning of Article 22; the intention is, precisely, to have significant negative effect on the attacker by preventing him from benefiting from his crime (there should also be significant positive effects on his intended victims). However, despite "ensuring network and information security" being declared a "legitimate interest" in GDPR Recital 49, and the use of state-of-the-art defence technology being required by the Working Party's draft guidelines on breach notification [4], these draft guidelines on automated processing make it unlawful (For how incident response should be conducted under Article 6(1)(f) see "Incident Response: Protecting Individual Rights Under the General Data Protection Regulation [5]", (2016) 13:3 SCRIPTed 258). This confusion is likely to make organisations reluctant to deploy automated network defences. Human mediation, as required by the Working Party, would reduce both the number of attacks that can be analysed and the speed with which they are mitigated, giving attacks and their impact more time to spread. We would expect this to increase the number, severity and extent of personal data breaches.
3. Many universities are now incorporating learning analytics into their teaching activities. This analyses patterns of student activity – for example in their use of library and on-line materials, attendance at lectures, and self-reported study hours – and identifies students who may benefit from various kinds of personalised support. While Jisc's Learning Analytics Code of Practice [6]agrees with the Working Party that major interventions should be decided upon by humans, the technology also enables a wide range of lesser interventions (personalised reading lists, reminders when a student is falling behind their

peers, etc.). We would consider it a breach of privacy if all such notifications were reported to tutors for review; students have expressed a fear that such reports might influence their marks. Nonetheless, by failing to explain which automated decisions have "significant effect", the draft guidelines are likely to result in universities, concerned about data protection compliance, inserting human inspection into even these low-risk processes and decisions. Jisc has recommended that learning analytics be carried out under the Article 6(1)(f) legitimate interests regime, ensuring that such activities always protect students' individual rights and freedoms (see "A data protection framework for learning analytics [7]" (2016) 3(1) Journal of Learning Analytics, 91–106 and "Downstream Consent: A Better Legal Framework for Big Data [8]" (2016) 1(1) Journal of Information Rights, Policy and Practice). The Working Party's strong encouragement of human inspection is likely to undermine that protection and increase the intrusion into students' privacy.
4. More generally, many organisations across both public and private sectors have taken advantage of technologies to perform rapid initial screening of requests, for example to detect fraud or reject obviously ineligible applications. If organisations believe these decisions may exceed the "significant effects" threshold the draft guidelines will force them to revert to manual processes, greatly increasing delays for all applicants and costs for all organisations. With the guidelines suggesting that that threshold might be very low, these harmful effects will be widespread.

General effects of guidance

1. The draft guidelines offer three ways that organisations can adapt automated decision-making processes to comply with this interpretation of the GDPR: either have the decision validated by a human, obtain the data subject's consent or declare the processing to be necessary for a contract. As the examples above show, we consider that the first is likely to result in disproportionate intrusion into individuals' privacy: the second and third seem likely to encourage data controllers to claim consent or necessity in situations where they are inappropriate (for example employment and on-line advertising).
2. The draft guidelines seem to contradict two of the basic aims of the GDPR – to reduce the overuse of consent, and to facilitate the beneficial use of new technologies. We agree with the Working Party that automation can amplify the impact of decisions: however imposing a ban with uncertain scope will discourage the use of privacy-enhancing automation by data controllers that wish to comply with data protection law, but encourage privacy-risking automation by those that see non-compliance as an acceptable business risk.

Conclusion

1. Under what we consider the natural interpretation of the GDPR text, most automated decision-making would be subject to a prior (and continuing) balancing test under Article 6(1)(f) with individual data subjects having the right to demand a review of both the fact of processing (under Article 21(1)) and its outcomes (under Article 22(1)). This is in accordance with the Working Party's 2013 call for a mechanism [2] that "should not only take the scope of the basic right to data protection into account. It should also assess the interests of controllers and should comprise an analysis of possible and actual impacts of profiling technologies on data subjects' rights and freedoms" (p.4).
2. If enforced, this appears to us a sound regime for encouraging automated decision-making where it will benefit and protect the data subject and discouraging it where it

may cause harm. By now presuming that automated processing is always harmful, the draft guidelines appear likely to create the reverse effect.

3. We strongly urge the Working Party to return to its 2013 interpretation of Article 22 as creating a retrospective right of review, not a prospective ban, of automated decision-making. We consider this new interpretation harmful to data subjects, data controllers and the objectives of the GDPR. If the Working Party insists that the Article bans automated processing, its guidance must at least provide clear guidance and legal certainty on the extent of that ban.

Source URL: https://community-stg.jisc.ac.uk/library/consultations/2017-article-29-guidelines-profiling-and-automated-decision-making

Links
[1] https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf
[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf
[3] http://ec.europa.eu/newsroom/document.cfm?doc_id=47742
[4] http://ec.europa.eu/newsroom/document.cfm?doc_id=47741
[5] https://script-ed.org/?p=3180
[6] https://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics
[7] http://dx.doi.org/10.18608/jla.2016.31.6
[8] https://doi.org/10.21039/irpandp.v1i1.9