Van: **Sergej Katus I PMP** sergej.katus@pmpartners.nl
Onderwerp: Comments on draft guidelines 01/2022 (data subject rights)
Datum: 2 februari 2022 om 20:38
Aan: EDPB

Dear EDPB,

I welcome your Guidelines 01/2022 on data subject rights and the opportunity to give comments.

I have two issues which I would like to bring under your attention. They stem from practical experience as a DPO for Dutch municipalities.

Please contact me if you have any furthers questions or need clarification.

Kind regards,

Sergej Katus

S.H. Katus, LLM CIPP/E CIPM FIP
Partner

PMP
Vondellaan 58, 3521 GH Utrecht
The Netherlands
E: sergej.katus@pmpartners.nl
T: +31 85 401 38 66 | M: +31 6 52 41 03 88
W: www.pmpartners.nl

---

1. Abuse of rights
Legal representation as such is correctly addressed on p. 27 of the draft guidelines. What seems to be missing is a paragraph on legitimate non-legal representation (e.g. a data subject authorises a trusted friend or family member to exercise rights for good reasons such as serious illness or other physical limitations).

What representation is concerned, I experience a special kind of abuse: specialised service bureaus that have made it their business model to target municipalities with access requests. These bureaus do not seem to provide sincere legal assistance to data subjects (in fact it should be easy for data subject to exercise their rights without hiring legal assistance). They just want to make make money - especially by catching the data controller in a mistake. Or even better; hoping for a refusal because that offers new opportunities under the Dutch General Administrative Act (see point 2 below). Requests in return by the data controller to narrow an article 15 request down to the information that the data subject really needs, are typically refused by stating that their clients request all personal data.

The GDPR offers the targeted municipality no protection. The requests these bureaus submit, may run in the dozens, while each request in itself is legitimate and not excessive in the sense of article 12.5 GDPR. On average, a civil servant who handles these broad requests, needs 40 hours per request for proper delivery. Failure to do so will immediately lead to the kind of escalation I describe under point 2.

Drivers may even be shadier. GDPR data subject rights may well play into the hands of organised crime as a means to gather intelligence or to impede the functioning of public authorities. For example, as a DPO I had to deal with a complaint from a petty criminal (he was quite open about that) for which in itself I had a lot of sympathy. At the same time, his complaint was closely linked to an acute drugs related public order and safety problem, police investigations and criminal proceedings aimed at someone else - apparently the key figure in all this. I recognised the name of this latter person from exercising his access rights through a service bureau (leading to a court procedure in the way I mention under point 2). In the meanwhile it appeared to me that the complainant I was currently dealing with, the petty criminal, was almost too well informed about his rights under the GDPR - to the extent that I got the feeling that I was being played.

2. Infringement of article 12.4 GDPR
I mentioned the Dutch General Administrative Act, which is relevant to the legal effect of the GDPR because of the deviation it causes from article 12 GDPR. After all, section 4 clearly states that, in the event of a refusal, an applicant must be able to apply directly to the national supervisory authority or the courts. Not so in The Netherlands, at least what the public sector is concerned.

The problem is article 34 of the Dutch GDPR Execution Act (UAVG), which states that any decision with regard to the exercise of data subject rights, must be regarded as an administrative decision according to the Dutch General Administrative Act.
This link blocks the legal protection and direct effect of Article 12 GDPR because it disregards the sui generis character of an article 12 decision, with its own mechanismes for legal protection as mentioned in article 12.4. The Dutch General Administrative Act provides for a whole different kind of procedures - the procedures for objection and appeal in which, among other things, an administrative objections committee plays a role (not the DPO and not the National Supervisory Authority, although court access is offered in the end.

Data subjects experience all this as a legal trap, because requests get entangled in often lengthy and more complicated legal procedures. Instead of a matter of months it may become a matter of years. Currently I am dealing with a complaint that has escalated to the court stage of the whole procedure, just because the complainant exercised her GDPR rights - basically her right to be forgotten - roughly one year ago and was wrongly refused.

I proposed the following solution for better direct effect of article 12:

1. People at service desks of public institutions must be trained to recognise and adequately respond to data subject requests - also in cases in which requesters do not explicitly invoke the GDPR. Any request is dealt with within one month or is refused with reasons.
2. In the case of an intention to refuse while substantial interests are at stake, the DPO must be involved in a timely and proper manner - to enable the data controller to decide wisely.
3. In any actual refusal (possibly not following the advise of the DPO) the reasons for refusal must be explained in an easily understandable and comprehensive manner. The refusal includes the information that if the requester disagrees with the refusal, he/she has the possibility to contact the DPO within one month, in order to obtain an independent expert assessment, hopefully leading to the quickest solution - without prejudice to the right to file a complaint with the National Supervisory Authority or appeal to the courts directly.
4. In case of a direct complaint with the NSA, it is most efficient that the NSA contacts the DPO for article 39.1d GDPR cooperation.
5. In any case, DPO's assess refusals within a month, which is regarded as a complexity in the sense of article 12.3 GDPR, thus giving the data controller time to correct mistakes within the timeframe of article 12 GDPR.
6. At the latest within three months, either the request is granted, or the requester is in the possession of a substantiated refusal that is accompanied by a DPO assessment. He can submit these to the National Supervisory Authority or the court, who can now make use of the DPO's expert opinion. In fact, the DPO will probably already have shared his/her conclusions with the NSA, lightening its workload as well.