PRIVACY COMPANY

OPEN LETTER

European Commission
Didier Reynders
Commissioner for Justice
Rue de la Loi / Wetstraat 200
1049 Brussels

The Hague, 19 December 2019

Subject: Ten suggestions for improvement of the GDPR

Dear Didier Reynders,

On behalf of the Dutch specialised privacy consultancy company Privacy Company I would like to contribute to the upcoming evaluation of the GDPR, based on our experiences as advisors for many small and large size organisations in the public and in the private sector.

We have ten pragmatic proposals to make compliance with the GDPR easier. Some of these suggestions correspond to the proposals of the joint German data protection authorities and the Dutch government. We summarise those proposals at the end of this letter. Overal, we want to stress that the GDPR works well, but we see opportunities to improve the effectiveness of supervision and to strengthen support for compliance with the privacy rules.

We would be very happy to provide further explanations, if you wish so.

Kind regards,

Frank Koppejan
Managing director Privacy Company

The GDPR works

Everywhere privacy officers have started to map existing processing operations, have conducted risk analyses and rolled out awareness campaigns. The GDPR has accomplished that personal data are much better protected than they were two years ago, and that compliance risks are high on the management agenda. In order to further increase support, the Commission can improve the GDPR in a number of areas, especially when it comes to the effectiveness of the supervision.

Good recommendations German DPAs and the Dutch government

We endorse many of the recommendations made by the German DPAs and the Dutch government. Our clients are also struggling with the extent of the right to a copy in case a customer files a data subject access request. We are affected by the large differences of opinion between the DPAs in their guidance on legitimate interests and direct marketing. Finally, we see a great deal of added value in the creation of legal privacy liability for manufacturers of devices and software that can be used to process personal data. It is impossible for most organisations to negotiate with international manufacturers themselves that they have to provide their devices and software in a privacy-friendly manner by default and permanently ensure a high level of security.

Ten suggestions for improvement of the GDPR

Apart from those suggestions, we have ten suggestion for the European Commission to facilitate compliance with the GDPR.

1. **Transparent decision-making**

We advocate a statutory publication requirement for all decisions from the DPAs. This allows everyone to learn from the explanations about the open standards. At present, a legal case against publication can sometimes take years and in fear of such litigation DPAs publish almost nothing. In order to understand how the GDPR should be applied in practice, it is essential that data controllers and processors worldwide be able to acquaint themselves with as many practical assessments as possible, even if it concerns a decision to reject a complaint because the DPA does not consider the complaint to be well-founded.

2. **Knowledge sharing via English translations**

We also advocate a legal obligation for the DPAs to translate any decision into English within a short period of time and to publish the decisions on the website of the European Data Protection Board. The Board or EDPB already publishes a limited number of decisions taken by DPAs, but this seems to be based on voluntary participation by DPA spokespersons. Any person affected by the GDPR and any organisation should have free access to all relevant explanations from a single central source. This source should be searchable on several criteria, such as the legal articles assessed and the nature of the sanction. This has the additional advantage that the DPAs can also coordinate their explanations better among themselves.

3. **Simplification of data breach reporting**

It is incomprehensible that all DPAs use their own ways and forms to report data breaches. We wholeheartedly agree with the Dutch government's contribution that there should be a single uniform digital form, but we find it even worse that a data controller has to fill in each form manually. This takes a lot of time and undermines support for the GDPR. The inefficiency of the process can result in some organisations deliberately not complying with the law. It creates frustration for organisations that spend a lot of time on careful reporting and increases the risks for data subjects who may not be

informed that their data have been leaked. The European Commission should therefore ensure that there is a single uniform reporting form that can be filled in automatically via an API. It is too early to raise a higher threshold for reporting data breaches at this stage, as proposed by the German supervisory authorities. First of all, the process needs to be improved.

4. **Knowledge sharing about data breaches**

The obligation to report data breaches was of course not created in order to increase the administrative burden for organisations. The data breach reporting requirement should be a tool to raise awareness about the risks of unlawful access to personal data and to share knowledge about the measures that organisations can take to reduce these risks. Such practical, applicable knowledge is invaluable, especially for SMEs. In order to achieve the higher goal of the requirement to report data breaches, DPAs should share much more knowledge about reported data breaches and measures taken, and about the considerations when organisations should or should not report a data breach to data subjects. Moreover, in the case of current incidents, this information should be shared with national alertness organisations such as CERTs.

5. **Clarity about cookie walls**

The European Commission must provide clarity about cookie and payment walls in the GDPR, now that it is apparently not possible to set clear rules in the ePrivacy Regulation. After more than two years of negotiations, the member states in the Telecom Council have not come one inch closer to each other when it comes to cookies and similar tracking technology, such as the use of pixels (beacons) in newsletters. The latest proposal for a new ePrivacy Regulation fell at the last minute at the beginning of December and nobody knows what to do next. The DPAs give very different explanations. For organisations that do their best to comply with the GDPR, it is unclear what they can and cannot do in their consent questions about tracking cookies. Can you ask visitors to use settings to deselect more than 40 different advertising networks one by one? Are you allowed to seduce people with a large YES button and a tiny link to 'change your settings'? Can you force people to pay if they don't want to consent to tracking cookies? As privacy advisors, we don't know where the boundary lies. See also our blog Tear down that cookiewall!

6. **Standard data processing agreement**

The European Commission can remove an enormous administrative burden for organisations by developing a standard data processing agreement, based on the current Standard Contractual Clauses for the transfer of personal data to countries without an adequate level of protection. The Commission can offer a checklist with a black list of prohibited clauses. Article 28 of the GDPR contains a large number of obligations for data processors. For example, that they may only process personal data on documented instructions from the data controller, that they may only use sub-processors with the data controller's written authorisation, that they must cooperate with audits and that they must assist in the performance of DPIAs. But reality is stubborn. Largescale cloud providers impose their own terms and conditions. For example, they ensure that the documented instructions from the data controller are equal to the content of the conditions drawn up by the provider itself, and the data controller can only withhold authorisation by terminating the contract. The EDPB has recently approved a data transfer agreeement proposed by the Danish DPA. However, even this improved version is not sufficient to (re)gain control over personal data. Bottlenecks are for example the cost allocation to audit compliance with the provisions of a contract. The Dutch Ministry of Justice and Security, together with the EDPS, is considering uniform European purchasing terms for cloud services at least for government organisations. But here lies a clear task for the European Commission, to simplify compliance for

businesses and organisations outside the central government with a standard data processing agreement.

7. **Scientific and statistical research**

The Commission should clarify the exceptions for scientific and statistical research (in Articles 9(4) and 89 of the GDPR). It helps to delete the second sentence from recital 159. This sentence states that the concept of scientific research should be interpreted in a broad manner, to include applied research and privately funded research. In practice, this leads to legal uncertainty. Are organisations allowed to conduct research into medical data for commercial purposes without the explicit consent of patients? Should social media, conversely, open up their *big personal data* to scientific research? And if so, can you, as data subject, object against such processing? The answer to this question is closely linked to the question of whether the data is pseudonymous or anonymous. As advisors, we often refer to the guidelines of the regulators on anonymisation and to the explanation of the Dutch national statistical organisation CBS on protection against identifiability of statistical data. However, these two guidances do not lead to the same conclusions. The guidance should therefore be harmonised at European level. In any case, the GDPR could explain in a recital that data can never be anonymous as long as the source data are still available or regularly become available again, and as long as the 'anonymised' data can still be linked to the source data, by the provider, by the recipient or by any other third party.

8. **Use of privacy labels**

The European Commission has been given the opportunity in the GDPR to develop standardised icons to provide data subjects with a meaningful overview of the intended processing through easily visible, intelligible and clearly legible manner. But these icons do not (yet) exist. Privacy Company itself, together with designer Tijmen Schep, and thanks to financial contributions from SIDNfonds, ECP and SURFnet has now made a first move with the Privacy Label. Any organisation who wishes to do so can use this tool to create a free visual representation of the most important elements of its privacy policy. But it would be even better if there were one standardized set of symbols, or guidelines with which such labels would have to comply. Organisations can then be more confident that they comply with the requirement that they provide the most important information at a glance, in an understandable manner.

9. **Public annual privacy accounts listed companies and government organisations**

In fact, every organisation with a Data Protection Officer should write an privacy annual report as part of the permanent internal focus on compliance. But the Commission must put the heaviest administrative burden on the strongest shoulders. Listed companies and government organisations already have a great deal of experience in the management of compliance with open standards, such as objectives in the field of corporate social responsibility. There should be a statutory requirement for these organisations to publish an annual privacy account in which they account how they have governed compliance with (international) privacy laws, how often the topic has been discussed at the highest management level, how many FTEs and how much budget they have spent on compliance, what successes they have achieved, how many data breaches they have reported to the DPA, what risks they have identified and what milestones they want to achieve.

10. **Reclaiming digital sovereignty**

We support the Dutch government's efforts to investigate the possibilities of curbing the data power of large tech companies through the GDPR. The idea of introducing new enforcement instruments for the DPAs, such as the stationing of an employee of a DPA at a large tech company, appeals to us, but these are relatively small steps. We encourage the European Commission to develop bottom-up new

strategies to regain digital sovereignty and to be able to effectively compete. There is ample knowledge in the Netherlands and Europe in the field of the technical development of hardware and software, (technical) public administration, digital ethics and privacy and competition law.

Appendix A: Key issues GDPR German DPAs

The regional German DPAs, united in DSK, have identified nine key issues with the GDPR in a letter to the European Commission

1. **Practical applicability of the GDPR**: easing the administrative burden by only providing information at the individual request of the data subject in the case of predictable processing, clarifying the scope of the right to a copy in case of a data subject access request and abolishing the requirement to report DPO contact details to the DPA;
2. **Data breach notifications**: introduce a higher threshold for notifications to DPAs, only if the breach is likely to result in more than minor risks to the rights and freedoms of natural persons.
3. **Purpose limitation**: stricter explanation that a legal ground is required for every processing operation, and that further processing can only be compatible if carried out by the same data controller.
4. **Data protection by design**: extend the scope of this duty to hardware and software manufacturers/suppliers. The German regulators specifically mention Windows 10 and Office 365 with reference to the DPIA reports of Privacy Company for the Ministry of Justice and Security.
5. **DPA powers**: remove the current limitation on DPA enforcement powers to cases involving processing operations. Allow DPAs to intervene in cases of non-compliance with obligations such as maintaining a record of processing activities, or appointing a DPO or representative.
6. **Mutual cooperation and consistency between DPAs**: clarify the circumstances in which DPAs must follow the coherence mechanism and increase the time limits to respond.
7. **Legal ground for direct marketing**: clearer explanation by the European Commission, because each Member State applies different rules. For example, whether an organisation may pass on customers and address details to third parties for direct marketing purposes on the grounds of its justified interest (other than e-mail addresses or telephone numbers);
8. **Profiling**: extension of the scope of article 22 of the GDPR to include a general ban on data processing for profiling purposes, with the only exceptions being a legal obligation, consent or performance of an agreement.
9. **Accreditation**: The German DPAs ask the Commission to settle a power struggle with the national accreditation body. The DPAs believe that they are the only ones competent to approve of a body that monitors compliance with a code of conduct.

Appendix B: Key issues GDPR Dutch government

From the letter of Minister Dekkers of 31 October 2019 to the Lower House.

- Reduction of the obligation for small businesses to keep a record of processing activities in order to reduce the bureaucratic burden on them;
- Avoid the extraterritorial effect of national implementing laws in order to avoid a new patchwork of legislation for internationally operating companies;
- Unification of the age limit when children can consent to the processing of their personal data
- Research into ways of further curbing the data power of large technology companies through the GDPR, for example by extending the possibilities of data portability and possibly by introducing new supervision powers for the DPAs;
- Make the facultative nature of a monitoring body explicit when using a code of conduct;
- Promote certification at EU level where possible and certification at national level only if it has real added value, and
- Promote the development of a single uniform form for the reporting of data breaches to the different DPAs of the Member States.

In its contribution to the Council of Ministers, the Dutch government mentions three other points of attention for the European Commission, namely:

- Big data analysis and profiling;
- Price discrimination through profiling;
- Blockchain and the probably insurmountable tension with the GDPR.