LEGAL UPDATE

Recommendations of Dutch Data Protection Authority for privacy policy

Date: 24 April 2019

On 17 April 2019, the Dutch Data Protection Authority (hereinafter "DPA") published recommendations for the privacy policy of organisations.

Article 24 of the General Data Protection Regulation (hereinafter "GDPR") requires organisations to implement a data protection policy depending on the nature, scope, context and purposes of the data processing. The DPA is apparently of the opinion that this policy should be recorded in writing and that a data protection policy will help the organisation to identify and take responsibility for all processing of personal data. According to the DPA, it is particularly important for organisations that process special and sensitive data to draw up and apply a good privacy policy.

The DPA bases its recommendations on its exploratory research into the policies at various organisations. The DPA found many differences in the nature and scope of the documents used at these organisations, and as no requirements are laid down in the GDPR about what form a data privacy policy should take, the DPA considered these recommendations necessary.

The six recommendations are as follows:

1. Assess whether the organisation is required to set up a data protection policy: not every organisation is required to do so. This depends on the data processing or the type of organisation.
2. Use internal and/or external expertise: the Data Protection Officer can play an important role in this as an adviser and internal supervisor.
3. Record the policy in a single document: avoid fragmentation of information in a privacy statement, a data processing register and a policy.
4. Be concrete: a data protection policy is a concrete translation of the GDPR standards in the context of an organisation's data processing. Reiterating standards from the GDPR is not sufficient.
5. Communicate the policy: while publishing the data protection policy is not mandatory, it gives data subjects insight into how an organisation deals with personal data. However, be careful with information about security when publishing the policy.
6. Even when publication is not mandatory, it is nonetheless advisable: through a data protection policy, an organisation demonstrates its commitment to protecting the personal data of data subjects.

The DPA is also of the opinion that a privacy policy should include the following: the categories of personal data, the purposes for which they are processed and the policy on dealing with the rights of data subjects.

The DPA's recommendations raise many questions. The categories of personal data and the purposes for which these data are processed are subject to change, which means that a policy would have to be frequently amended. This is impractical in (large) organisations where many people are affected by the policy and there is a need for policy consistency. Instead, it would be more practical to refer to the data processing register in the privacy policy. Furthermore, it is illogical include a privacy statement in a privacy policy.

A privacy policy indicates who has what responsibilities within the organisation and how the policy is monitored. It also provides guidance to employees when processing personal data (e.g. which persons should be involved at which stage in case of a data breach, and whether a data processing agreement can be concluded with third parties without a prior review by the Legal department, and if so, which agreement). By contrast, the purpose of a privacy statement is to explain to data subjects how personal data are dealt with. An organisation often has different privacy statements for different groups of data subjects relating to different activities. By putting everything in a single document, an organisation risks that both the employees processing personal data and data subjects will not read the policy because they feel it does not concern them. It is actually very advisable not to impose any formal requirements for a privacy policy, because every organisation faces different challenges. For some organisations it is useful to have an extensive policy on the rights of data subjects, but this issue is far less relevant in other organisations, which therefore don't need an extensive written policy on this. Lastly, publishing a privacy policy is not always an obvious step, as it can actually have negative consequences for the security of data processing.

In short, it is good to take the DPA's recommendations into account when drawing up policy. However, it is advisable to remain critical and to only follow the recommendations in so far as this has a positive effect on data protection within the organisation.

This is a Legal Update from Elze 't Hart, with thanks to Anne van der Sangen.

For more information:

Elze 't Hart
+31 30 25 95 578
elzethart@vbk.nl