contrast

YOUR BUSINESS • MAY 2021

GDPR in (a checklist of) 10 points? Yes, we can!

What you need to know.

The GDPR entered into force exactly 3 years ago, on 25 May 2018. Many companies began implementing the GDPR around that time, but can no longer see the forest for the trees. Other companies do not know where to start at all. And those companies which did complete the exercise at some point grow discouraged when they think about evaluating and updating the first exercise.

Is this an exaggeration? Certainly not! The 88 page GDPR counts 55,000 words, set down in 173 considerations and 99 articles. Identifying (all of) the concrete obligations deriving from this massive text is no easy task. But there are tools!

Several national data protection authorities have already published a number of useful ones: from GDPR roadmaps (e.g. from the French CNIL *[currently only available in French]*) to concrete models (e.g. the processing agreement from the Danish Datatilsynet). It is therefore certainly useful to consult the authorities' websites. However, a complete, and at the same time concise and really practical, overview that allows one to systematically check all obligations under the GDPR, is still lacking. And that is why **contrast** has drawn up a checklist of 10 points.

What you need to do.

If your company has not (yet) mastered the GDPR, rest assured that you are certainly not alone! It is not too late to start, continue or update the GDPR exercise. Nor is it an impossible task. At **contrast**, we use the following 10-point checklist:

1. **Purpose**: start by identifying the different purposes for which your company processes personal data. Put this question to the various departments within your company: HR, sales, marketing, etc. You can already give them some inspiration by providing them with a list of common processing purposes (with a concrete description). On the basis of these purposes, your company will determine which personal data are necessary and how long your company is allowed to keep them.

2. **Ground**: for each of the purposes, identify the most appropriate legal ground in accordance with

Articles 6 to 10 of the GDPR. This is a task for lawyers in consultation with the employees who are responsible for processing within your company. Depending on the chosen basis (consent, legitimate interest, etc.), additional actions may be required.

3. **Rights**: check whether the identified purposes (and all related information according to Articles 13 and 14 of the GDPR) are included in a privacy statement for the data subjects. Does your company process personal data via its website? If so, a privacy statement on the website is necessary. Does your company decide to make a list of its employees' birthdays in order to send birthday wishes? Then you should check whether this is included in the privacy statement for employees. Furthermore, it is important to provide procedures for answering requests from data subjects in accordance with, amongst others, Article 12 of the GDPR: is an absolute opt-out for direct marketing provided, who will answer an access request, how must a data subject prove his identity, which (response) models must be used, etc.?

4. **Third parties**: for each of the purposes, identify the third parties who have access to/use the personal data. Let a legal expert help you qualify these third parties as processors, joint controllers or separate controllers. Do not lose sight of group companies! Depending on the qualification, you should verify whether the necessary (contractual) documents are in place.

5. **Third countries**: check whether these third parties are outside the European Economic Area or are subsidiaries whose parent company is outside the EEA. If that is the case, your company must take the necessary safeguards to ensure an equivalent level of protection in the relevant third country. Again, lawyers can help with this.

6. **Security and data breaches**: depending on the risks involved in the processing, check whether the current security/what security is appropriate to protect the personal data against unauthorised access, loss and alteration. The risks (and thus the steps to be taken) will depend on the types of personal data that are processed, which technologies and infrastructure are used in the context of the processing, etc. It is advisable to call on (IT) security consultants for this. It will not be possible to completely eliminate every risk. It is therefore important that your company also take measures to identify data breaches, document them internally and report them to the concerned authority and data subjects involved.

7. **DPO**: verify whether (one or more of) the purposes will require you, as a company, to appoint a *data protection officer* and notify the concerned data protection authority(ies).

8. **DPIA**: verify whether (one or more of) the purposes involve a high risk for the data subjects. You can do this analysis on the basis of e.g. the lists published by the data protection authorities or on the basis of the criteria of the European Data Protection Board. In case of a high risk, you should perform a data protection impact assessment (a type of impact analysis) and possibly obtain prior approval from

the data protection authority concerned.

9. **Policies and procedures**: even if your company is not required to formally appoint a DPO, at least make sure that *someone* is centrally responsible for monitoring GDPR compliance within your company. Also be sure to raise awareness and properly train your staff. Furthermore, every company must in any case have a procedure for responding to requests from data subjects, for documenting and reporting data breaches, for deleting personal data and for correctly securing such data (e.g. per data system). The register (see below) can be a useful tool for this. It is also prudent, for example, to integrate the use of this checklist into the standard procedures for the start-up of new projects.

10. **Records**: ensure that the information collected in the context of this checklist is included in a record of processing activities in accordance with Article 30 of the GDPR.