Docuware

A GDPR To-Do List

General Info

14 measures you should take in advance of the General Data Protection Regulation

It’s coming soon: Companies must be ready for the General Data Protection Regulation (GDPR) by May 25, 2018, as it will apply then Europe-wide. Attorney Rolf Becker, partner at Wienke & Becker, Cologne, provides concrete tips in the form of 14 measures you would be wise to implement immediately so that you are prepared. The devil is in the details and requirements in terms of the design of a data protection management strategy.

Meeting the reverse onus head on

Up to now, in the event of a complaint or data incident, the onus was on the data protection authority, for example, to prove to you that something had gone wrong in your company's organizational management process. However, with the imminent application of the GDPR, this is fundamentally changing. If, in this case, you cannot prove that the data was indeed processed in compliance with data protection legislation, you have a problem. This problem is borne out most starkly in the threat of penalties of up to EUR 20 million or 4% of global revenue, whichever is higher.

Proof is furnished, in the first instance, by evidence of strict compliance with the obligation to document your data processing operations. You must be able to prove compliance with the principles governing the processing of personal data, for example, personal data must:

- be processed in a lawful manner, in good faith, and in a way that is traceable for the data subject;
- be collected for defined, unique, and legitimate purposes and must not be further processed in a way that is not reconcilable with these purposes;
- be factually correct and, where necessary, be fully up to date; all reasonable measures must be taken to ensure that any personal data that is incorrect in relation to its intended processing purpose is deleted or rectified immediately.

Are there exceptions?

This is always the first question people ask when looking for a loophole to sidestep the requirements. Such loopholes do exist but very few companies manage to exploit them successfully. It's only if you employ fewer than 250 staff and “only occasionally” handle data processing operations in your business (which automatically rules out all mail-order companies, for example) that you have the possibility of getting away with fewer obligations. Even then, specific risks, or the processing of sensitive data such as account data, could become grounds for enforcement of the full set of obligations.

14 measures you should take now

In terms of the approach you should take, we can only provide a brief outline of important topics but due to their scope we advise you to review the complete set of requirements for the GDPR. Here are 14 measures we recommend:

1. Within your company, **put together a team** drawn from the divisions in which data is collected (e.g. HR department, payroll accounting, customer service, shipping/logistics, advertising department, IT). Make sure to include a data protection officer right from the start. Get the works council involved.

2. Identify the **areas that are relevant for data protection law** and agree on the approach to be taken to document individual data collection operations, their purpose, relevant permissions, and the deletion of any data collected. Think also about candidate management, your travel expense accounting system, key management, time recording, email system, supplier management, warehouse management, video monitoring, firewall, social media policy, loyalty card programs, tracking measures, forms of direct advertising, personalized advertising, etc. The obligation to document applies to all departments that handle personal data. It also applies to your employees’ unofficial hardcopy lists and Excel tables, which should be gotten rid of as soon as the task at hand is complete. In particular, your employees’ own hardware can entail considerable data protection problems and risks.

3. In this context, it is important to create registers of procedures—or to use GDPR terminology “**records of processing activities**”. Based on the documented description alone, these procedures can be used to ascertain whether the entire process—from data collection right through usage and deletion—is being carried out in compliance with data protection legislation and to determine what measures are to be taken to ensure compliance (**actual/target analysis**). All processes that are relevant for data protection should be documented in the records of processing activities, which the authorities can request to inspect.

4. A record of processing activities can **also be maintained electronically**. Special software is available that provides structures and prescribed content to make this task easier. Your record of processing activities should include information such as details regarding those in charge, the processing purpose, the categories of data subject, data, and recipient, details on transfer outside of the EU (e.g. for trackers), details regarding deletion and the description of security measures (Technical Organizational Measures, so-called TOMs).

5 You should identify the **legal basis** underlying the respective usage straightaway. This is either legal facts, such as the performance of a contract, or consent. **Document the consent texts** and the processes in place for obtaining consent and for archiving, and have these **checked for compliance with the regulation**. Keep a record of which **information was communicated for each data collection** activity and have this legally checked for adequacy.

6 Create a **monitoring strategy**: How, when, and how frequently spot-checks can be performed on the consent texts to ensure that they match the entries in your software? What other security measures are being taken? The intention of the law is to ensure that you implement a **data and security management** system now, and maintain it into the future. There is a particular focus on **IT security**. You must collate all IT security measures that you have taken or that you intend to take. This starts with access to offices and the server room and doesn't necessarily end with the firewall. Collating all of the relevant facts and documenting them in a way that allows them to be maintained in the future and adapted to changes is a particular challenge. The German Federal Office for Information Security (BSI) has made available a checklist.

7 You need to be able to prove through documentation that your company has established procedures and rules (guidelines, processes, etc.) that permanently define, manage, monitor, and improve information security. Proof of legally compliant management procedures can also be provided by means of **certifications**. Think about such certification early on, and make sure that it complies, as much as possible, with the GDPR, at least in terms of IT.

8 In particularly critical areas, you need to implement a **data protection impact assessment**. This applies when the data processing entails a high risk for the rights and freedoms of natural persons. The EU data protection group (Article 29 Group) has defined ten criteria which, if fulfilled, indicate that such a risk exists. Each data processing operation must be checked in advance to determine whether it is likely to involve such risks. You should then record the result in your register of processing operations.

9 Create a response plan for data breaches. Every cyber risk insurance policy, something you should have in place, makes provision for risks of this type. Keep a record of:

- who should be alerted by whom and when,
- what immediate measures must be taken,
- what must be documented, and
- how the information and reporting obligations to the authorities are to be implemented.

Cyber risk insurance policies provide protection in the event of data breaches.

10 Clarify who in your organization is responsible for ensuring **fulfillment of the rights of data subjects**. Make sure that specimen answers and employee training are provided. In collaboration with the IT department, define which data records are to be compiled and in what way, as well as the form (electronic especially) in which they should be made available to the data subject if requested. As part of this process, define which data can be subject to restricted processing, deleted or blocked on request, and which data must be archived. Check what processes and strategies are in place for **handling contradictions in advertising** and document this in your register of processing operations. Define how the **correctness of data** can be verified.

11 Check the effects of the new "**right to be forgotten**". In what areas of your company is the data of data subjects forwarded to third parties (e.g. press release with photos and names of competition winners)? Who would you need to inform if the data subject wanted to assert their right? How can you avoid that? The same applies to the right of data portability, which can require you to forward certain data to competitors at the request of the customer.

12 Update your **contract management** system. All contracts with service providers in which personal data plays a role must be legally checked for compliance with the new data protection requirements. The law requires contract data processing agreements with very specific minimum content.

13 Finally, address **employee undertakings** in relation to data confidentiality. Existing undertakings are no longer sufficient and must be renewed at least once a year in any case. Employees should now be bound to confidentiality for evidence reasons, even if the law no longer recognizes an express undertaking outside of the public sector.

14 In collaboration with your data protection officer, organize regular **training sessions and awareness initiatives** for your employees.

Summary

Although this does not necessarily cover all of the tasks to be carried out, it does provide a good outline of the important steps you need to take in order to ensure that your company is GDPR-ready, and to ensure that you can provide proof that you have fulfilled all of your due-diligence requirements. Fines are expressly intended to have a deterrent effect in the future. Get support from specialized companies, who can also appoint a data protection officer for you and provide you with the accompanying legal advice from specialized attorneys.

Docuware

For more information please visit our website at:

www.docuware.com