FACTSHEET - DATA PRIVACY

In control of privacy risks?

Legislation and regulations in the area of data privacy are subject to constant change. At the moment, this can be seen in the obligation to report data breaches, the Dutch Data Protection Authority's increase power to impose penalties, and the upcoming General Data Protection Regulation (GDPR) in 2018. To provide our clients with the best possible service, at BDO, we have combined all of the knowledge and expertise on privacy we hold in different domains, such as cybersecurity, legal and audit. BDO has designed a programme to help organisations prepare for compliance with the stricter data privacy legislation:

Step 1: Determining a privacy strategy

What is your strategy and what are your objectives in relation to data privacy? We will conduct an interview with you to find the answer to this question.

Step 2: Performing a privacy scan

An assessment provides information on the risks in the area of data privacy within your organisation. The risks are used to determine the measures that are relevant for your organisation and the extent to which you have already taken the right data privacy measures. We do so on the basis of the following steps:

Gap analysis
We start by performing a gap analysis at organisations that have little or no experience in the area of data privacy. We assess which data privacy measures are inadequate or are missing, based on the requirements imposed by the GDPR and the organisation's risk profile. Subsequently, the improvements needed in order to address the chief risks are decided jointly with you.

Privacy maturity scan
If you have worked on data privacy for some time, your organisation will have a higher maturity level in this area. In that case, we will measure your privacy maturity level. We use an automated questionnaire for this purpose. Based on the results of this scan, we come up with improvements for you. You can monitor the results of your improvements by repeating the scan.

Step 3: Preparing and carrying out programme of improvements
Based on the outcome of the privacy scan, we work with your organisation to define a programme of improvements. The following activities or projects may form part of this programme of improvements:

Setting up a privacy organisation
Which changes need to be made to your organisation in order to manage data privacy risks? Do you need to have a Data Protection Officer (DPO)? Where is the best place for the DPO in your organisation, and which duties will the DPO have?

Compliance with provisions on documentation
We identify the documentation requirements that the GDPR imposes on your organisation and set up the necessary records. For example, we can set up digital records of the nature, size and security measures of your personal data processing operations and the length of time data are kept.

Data breaches
Data breaches can take many forms. They can be caused by something as simple as sending an email to the wrong recipient. We can assist your organisation with setting up effective procedures for detecting data breaches and dealing with them in accordance with the requirements imposed by law.

Data protection impact assessment (DPIA)
When you adjust your business processes or put new applications or IT systems into operation, you may need to carry out a data protection impact assessment (DPIA). Your organisation can use the DPIA to demonstrate that you take sufficient security measures when processing personal data in the new situation. A DPIA enables you to apply the principles of privacy by design and privacy by default. We can assist you with your DPIAs and help you adjust your change processes so that a DPIA is included as a matter of course.

Data processor agreements
As an organisation, you are responsible for complying with laws and regulations when personal data is processed, even if you use external suppliers to do so. We can assist you with drafting data processing agreements with suppliers. In addition, we set up processes that are needed in order to conclude such agreements and monitor compliance with the arrangements agreed with your suppliers.

Privacy statements and policy documents
Do your clients and employees have a clear picture of their rights under the GDPR? Is it easy for them to exercise these rights? Many existing privacy statements, agreements, internal policy documents and procedures do not comply with the requirements imposed by the GDPR. BDO can assist you with assessing, amending and/or drawing up the right documents and procedures.

Raising awareness of data privacy issues
Time after time, people turn out to be a crucial link in the management of data privacy risks, and BDO believes it is crucial that employees are given information on how they can help to protect privacy. We do this by preparing and implementing an awareness programme that is tailored to your organisation.

Demonstrably in control
Compliance with data privacy legislation and regulations is a constant process, and the effectiveness of the measures taken must be checked regularly. We can assist you in setting up the internal controls you need in order to be demonstrably in control with regard data privacy.

Step 4: Maintaining data privacy in the form of 'as a Service'

Once you have dealt with steps 1 to 3 and laid the foundation, there is still more you need to do. How do you actively manage data privacy while carrying on the underlying operations? As your organisation and environment will change, you will also have to adjust your existing measures to reflect these changes. To this end, you can make use of our consultancy services: the data protection officer (DPO) as a service, and the data breach officer (DBO) as a service.

Internal monitoring of compliance with privacy legislation

The introduction of the GDPR will result in many organisations having to appoint a Data Protection Officer who monitors compliance with privacy rules within an organisation.

BDO can offer you a certified DPO who knows all the ins and outs of the privacy rules, who is familiar with your specific situation and who performs the duties required by law for your organisation. The DPO can perform the following duties for your organisation:

- Maintaining and updating your data privacy procedures and policy documents;
- Monitoring compliance with the relevant data privacy legislation and regulations;
- Advising on issues related to data privacy;
- Acting as a point of contact for the regulatory authorities;
- Providing assistance with DPIAs;
- Providing assistance when making arrangements on personal data protection with external parties, including drafting and concluding data processor agreements;
- Providing support in dealing with suspected or actual data breaches.

Support in the event of a data breach

In the event of a suspected or actual data breach, we can address the data breach jointly with your organisation. The BDO data breach officer will investigate the data breach with your organisation and will ensure, on your behalf, that it is reported promptly to the competent authorities, such as the Dutch Data Protection Authority, and to the data subjects if necessary or desired. Should your existing data breach procedure be inadequate, we will modify this procedure in collaboration with you.

Further information

If you are looking for assistance in making the necessary changes relating to the upcoming GDPR, please contact the person below for a meeting without obligation.

Robert van Vianen
Phone (+31)6 - 300 79 909
Email robert.van.vianen@bdo.nl

10/2017 – AD1756