Factsheet
Organising Accountability

“Accountable for compliance with legal and contractual obligations”

Accountability obligations

Various laws have accountability obligations. The best-known example is the Tax Law. The European General Data Protection Regulation (GDPR) and the Medical Device Regulation (MDR) are other examples. Companies and individuals must promptly answer the supervisory authorities with reliable data to comply with the accountability obligation.

Supervisory arrangements

Statutory accountability influences the behaviour of companies, individuals, and supervisors. In tax law, incorrect accountability information leads to reversal of the burden of proof, estimates of taxable amounts and fines. In the GDPR, incorrect accountability information leads to liability risks and fines. The reversal of the burden of proof is already anchored in the GDPR with the mandatory reporting of data breaches. Both laws are based on a chain liability for the main contractor or controller.

The often mutually contradictory supervisory arrangements of the legislature create considerable administrative burdens and compliance uncertainty for companies.

However, acting according to relevant laws aligned, embedded in business processes and organising the company's accountability for compliance with the aligned legal and contractual obligations ultimately results in operational relief and more insight into liability and cost risks.

Added value

Compliant behaviour for the protection of personal data always supports the achievement of the company's objectives. We could even say that it is a prerequisite for it. Foreclosure and making agreements on processing company data protects this data, including trade secrets and the company's intellectual property.

Also, making agreements with individuals about their data processing leads to the legitimate processing of this data and allows the company to better approach its target groups.

The agreements impact the data quality, enabling the company to set up its business processes more effectively.

Taking control measures

By taking the right control measures accountability offers the company to better connect with target groups and reduce operating costs. The company accounts itself to civil society, particularly its partners such as employees, customers, and suppliers, about the effectiveness of control measures.

The company agrees on the objects' accountability and process towards accountability through the Trust Network, smart contracting and compliance with its partners. It is resulting in bilateral processing and consent agreements being unnecessary, saving both time and money.

Compliance approach

MYOBI is a trusted third party (TTP), maintaining a Trust Network.

On the Trust Network, business users have an Information ecosystem maintaining company and personal data and manages their legal and functional structures. Also, they conclude agreements with their partners on processing and sharing company and personal data.

Companies are accountable to civil society through the Accountability Seal Register on the appropriate processing of the shared data.

All users comply with the TTP policy obligations, which are summarised in the TTP rules.

The mechanism and compliance approach

Based on generally accepted accountability processes and guidelines, particularly from regulators, MYOBI has designed a practical compliance approach for companies. Companies can use the compliance approach for relevant legal and contractual obligations mutually aligned and apply it.

On the MYOBI Trust Network, the compliance approach focuses on meeting legal and contractual obligations for data protection and information security. The network's users' accountability

increases certainty about its reliability and personal data, which is a vital bycatch of demonstrating compliance with legislation. At the same time, reliable company and personal data are pre-conditional for organising effective business activities.

The board (the management) expresses policy and indicates to which extent legal and contractual obligations will be fulfilled. The policy gives rise to the establishment of appropriate technical and organisational control measures.

A compliance mechanism shall be set up by the company to measure and record the effectiveness of the control measures taken. This 'accounting' forms the basis for the management to justify itself to the civil society.

How does the mechanism work?

The Data Protection Officer (DPO) has a legal GDPRduty to advise the board upon data protection policy and appropriate and effective control measures. Also, the DPO oversees the register of data processes and privacy and security accounting. The DPO has an obligatory supervisory role, according to the legislator.

The board can assess compliance with the policy best based on the accounting of effective data processing and express results in a self-declaration. Mainly and if available, the DPO determines whether or not to confirm the self-declaration because of its (legal) position and role. If necessary (and possible), an internal Audit Office be involved as well.

MYOBI includes the management's self-declaration and the available confirmations in its plausibility investigation and adds the results to the Accountabi-lity Seal Register.

It is an annual cycle that is in line with the usual company's financial reporting. MYOBI organises the mechanism in collaboration with compliance professionals from Duthler Associates. There is an education and training portfolio for companies, professionals providing support, and MYOBI proposes practical workflows.

The civil society, in particular the company's partners, derives value from this Accountability Seal when processing data and doing business.

Accountability tools

The compliance approach makes and keeps the obligations explicit (expressed in standards; baselines). Partners collaborate on the Trust Network, and expectations on data protection must be unambiguous and clear.

Based on the mutually accepted TTP policy and a quality model (TTP Code of Conduct GDPR), partners control and direct their data on the Trust Network.

MYOBI has incorporated the TTP Code of Conduct GDPR into the Accountability Seal Policy as an interoperable "language" for complying with legal obligations to protect personal data. See Figure 2.

The Association VIE

The Association VIE (Association of users of Information Ecosystems on the Trust Network) has an essential role in establishing and maintaining the TTP Code of Conduct GDPR.

The TTP Code of Conduct GDPR is an essential part of the TTP policy, particularly the Accountability Seal Policy.

The Association VIE submits the TTP Code of Conduct GDPR for approval to the Dutch Data Protection Authority (AP). After AP's approval, the Information Ecosystem the VIE members enjoy clarity about what measures are appropriate.

Accountability Tools

A proactive organisation delivers the intended results of the compliance approach. MYOBI initiates and guides the Trust Network user through the accountability cycle primarily focused on being compliant with the TTP Code of Conduct GDPR.

MYOBI provides tools such as:

- A company-specific learning environment focused on employee awareness and knowledge transfer to key staff;
- Legal Entity Management provides an overview and insight into one's own and partners' formal and functional structure.
- Smart contracting for concluding processing and consent agreements company and personal data with partners; *and*

- Registers, such as the register of keeping data processes.

Company-specific learning environment

As part of the registration process, MYOBI creates a company-specific learning environment. MYOBI uses Duthler Academy's infrastructure for this purpose.

In collaboration with Duthler Academy, MYOBI manages a role-driven education and awareness portfolio aimed at building and managing its own Information Ecosystem. This portfolio makes Duthler Academy available in a company's learning environment.

Maturity levels

At the start of the accountability cycle, MYOBI supplies personal data protection and information security baselines, which allows a company to indicate the maturity levels: to what extent does the company meet GDPR management objectives. At the company's request, MYOBI examines to which extent sufficient observations have been made.

At the end of the accountability period – which may be equal to the financial reporting period –, the company's assessed and documented maturity levels are the basis for the management's self-declaration. In the Accountability Seal, the maturity level is adopted by the board and published in the Accountability Seal Register. MYOBI publishes the register on its website.

Role of the DPO

The Data Protection Officer (DPO) determines whether or not to confirm the self-declaration, which is part of the legal role of monitoring the company’s compliance with the GDPR.

Also, the DPO publishes the confirmation or abnormality of the maturity level in the Accountability Seal Register on MYOBI’s the website.

Self-declaration review

MYOBI completes the accountability cycle by performing a plausibility test on the self-declaration. MYOBI reports the results of the test in the Accountability Seal Register. MYOBI has developed the accountability cycle in several guidelines, enabling employees to apply the baselines, organise self-declaration, and support the DPO confirming management's self-declaration.

Boards’ Control

The structure of MYOBI facilitates and controls the Trust Network. The MYOBI is accountable for the Trust Network operations and enables professional services, such as smart contracting and smart compliance. MYOBI provides tools for users such as the baselines, guidelines, and training and performs plausibility tests on self-declaration.

MYOBI maintains two boards:

- Standardisation Board: responsible for managing and properly using sets of data definitions. Users of the Trust Network are mutually interoperable with the data definitions for processing (personal) data; *and*
- Monitoring Board: responsible for monitoring compliance with the TTP Code of Conduct GDPR. The Board gives requested and unrequested advice on the operation of the Code of Conduct.

The Monitoring Body is a supervisory body of the Association VIE and takes care of the Association VIE members.

Independent Association

The VIE Association mentioned earlier promotes the proper application of the GDPR's accountability obligation, which is a prerequisite for exercising control over personal and company data on a Trust network. Users need to be able to rely on the quality of data from the Information ecosystems.

To maintain and ensure the quality of data, it is crucial users being accountable for their compliance with the obligations of the GDPR. The TTP Code of Conduct GDPR is primarily intended to provide users with a framework and tools to fulfil their accountability obligation. Therefore, one of the VIE Association’s aims is to maintain and improve the Code of Conduct and promote the Code of Conduct application as a tool to comply with the GDPR's accountability obligation in a uniform and predictable manner. In this way, the Association helps to form interoperable compliance.

Members of the Association are:

- Companies, controllers and processors, accountable for processing and contributing to the conservation of Information Eco-systems; and
- Persons whose data is an object for companies using the Trust Network.

These companies and persons are always users of a TTP. Users of MYOBI Trust Network automatically become members of the Association.

Expectations

The AP focuses primarily on maintaining the GDPR and restricts giving advice.

For many organisations, data protection has so far been limited to arrange their obligations formally. Awareness of the employees has been central to this. Now the employees' attention is impairing, refreshment about data protection aspects is needed and organisations should - by design and by default - implement effective measures protecting (personal) data. See also the AP's policy for 2020 - 2023.

The organisation of data protection is also affected by national and international influences outside of the GDPR. We want to highlight the MedMij agreement system of MedMij.

The MedMij program enables patients to control and direct their medical data. The program of MedMij have led MYOBI to professionalise the Trust Network even further. The goal of MYOBI is to proactively support the Trust Network users in meeting legal and contractual obligations of data protection and information security.

By explicitly putting the companies' business activities first, MYOBI offers the preconditions to better align with their target groups and to organise business processes more productively.

TTP Code of Conduct GDPR

The TTP Code of Conduct GDPR is an integral part of MYOBI's compliance approach. The Code of Conduct facilitates the interoperability of compliance with legal and contractual obligations between users on the network. The Code of Conduct provides users with certainty about what control measures need to be taken to comply with GDPR obligations and understanding the liability and cost risks of non-compliance with the TTP Code of Conduct GDPR. The Association VIE intends to submit the code of conduct to the AP.

Timeline

The company's management keeps records of the manually process of organising the accountability for the compliance for the GDPR obligations. The same goes for the DPO. Many managers consider fulfilling this accountability obligation under the GDPR to be a struggle.

Companies' efforts will increase as both the European and national supervisors focus more on companies' supervisory tasks, particularly handling data breaches and other investigations. Also, there is an increasing exchange of personal data and outsourcing processing (going to the cloud with the data processing), which increases accountability pressure.

With the MYOBI compliance approach, we align the 2020 accountability for safeguarding personal data with the financial statement and the board report process.

In 2021, MYOBI will run a structured accountability approach focusing on performing plausibility checks confirming Accountability Seals.

Based on the outcome of the risk analysis, for each baseline objective, the company determines, the frequency of monitoring the control measures' effectiveness. This is about the risk that could have an impact on a data subject. It's about data processing where a data breach can have a major impact on a data subject's privacy.

With the help of the LEM Management, the company can assign goals/tasks to process owners. These owners delegate the execution to employees. A workflow supports the timely execution of the checks.

In carrying out the checks, the employee stores the evidence demonstrating the operation of the measures. The objective owner can then easily determine whether it agrees to the goals/internal audit objective.

The checking results during the year may lead to the company tightening up procedures, training (additional) staff, or taking additional measures. The DPO will also want to monitor the results of the checks closely.

Based on the results of the internal audits during the year, the company's management can make a statement to what extent the organisation has been able to comply with the TTP Code of Conduct GDPR. This statement or self-declaration expresses the maturity level of the company.

The DPO, which has monitored GDPR compliance throughout the year, adds confirmation to the self-declaration indicating whether the level of maturity is endorsed or whether the DPO has come to a different conclusion.

Both the management self-declaration and the DPO's confirmation are converted into an Accountability Seal and reflected in the Accountability Seal Register, which can be consulted by civil society. After carrying out a plausibility test, MYOBI adds the maturity level in the Register it has established.

Contact

Jetse J. Biesheuvel

j.j.biesheuvel@myobi.eu

+31 (6) 52 388 572

REGISTER