TaylorWessing

Compliant or non-compliant?
GDPR audits as a self-control tool

In order to ensure a high level of data protection within the EU, the GDPR provides for strict compliance responsibility on the part of companies processing personal data. As they are accountable by law, companies have to comply with the regulation and must be able to prove their compliance, e.g. upon request of the supervisory authorities. Respective inspections by supervisory authorities may occur on a case-related basis or without any particular reason.

If companies are unable to prove their compliance, they may face heavy fines. Record-breaking fines show that the supervisory authorities are not afraid to use their powers. In order to avoid these fines, it is not enough to singularly adapt internal processes to the legal requirements. Companies must constantly maintain the data protection standard they have created, especially since the GDPR is not yet a well-established legal framework. Therefore, the opinions of the supervisory authorities and the courts have a considerable influence on the interpretation of the legal requirements. As a result, the specific interpretation and prioritization of individual obligations under the GDPR has changed since coming into force - accompanied with a corresponding need for action.

Companies should therefore ensure that their data protection standards are put into practice internally, including in new projects. After more than two years since the GDPR entered into force, companies should critically review how they have implemented it. A GDPR audit may be a suitable tool for this.

If the GDPR requirements have not yet been implemented, a step-by-step implementation of the numerous data protection requirements is a viable approach. Please refer to our Step Plan GDPR implementation for guidance.

Advantages of a GDPR audit

There is no explicit legal obligation to carry out audits under the GDPR. It only obliges companies to carry out regular reviews of their technical and organizational security measures (e.g. through penetration tests) depending on the data processing risk (Art. 32 (1) (d) of the GDPR).

However, comprehensive audits can make it easier for companies to prove their GDPR compliance and to meet their legal obligations.

- On the one hand, the audit evaluates the internal implementation of the GDPR requirements and documents it accordingly. In the best case, this documentation can serve as proof of GDPR compliance to the supervisory authority. Even if the audit does not provide complete proof of compliance, the audit documents the corresponding efforts and will generally need to be considered in favor of the company when calculating a fine

- On the other hand, an audit can uncover internal errors and deficiencies of the GDPR implementation and thereby show companies their need to adapt to ensure full compliance. Even two years after the GDPR came into force, many companies have still not succeeded in fully implementing it, as is evidenced by high fines in the EU

In addition, audits offer a "reality check". Many companies were under time pressure when implementing the GDPR requirements. In many cases, processes were initially developed and guidelines drawn up, but the actual compliance with these in the day-to-day work of the company was often neglected. Frequently, the created standards have not been practised or have been implemented inconsistently. For example, if the internal IT systems are not adapted in accordance with the internal standards or data deletion obligations are not enforced, compliance only takes place on paper. Companies run the risk that these deficits will be revealed in the event of data breaches, data subject access requests or in the course of supervisory authority proceedings. Companies should avoid this in any case in order to avoid the risk of corresponding fines. An audit helps to evaluate whether the implemented measures were successful and have actually led to a higher level of data protection. Audits are thus an important means of self-control.

Internal or external audit?

It is possible to carry out GDPR audits both internally or externally. The goal of the audit determines which procedure should be chosen.

- An external audit is carried out by an independent body and is therefore best suited for obtaining objective proof of GDPR compliance

- An internal audit, on the other hand, is primarily suitable as a means of self-control. It can be used to verify whether GDPR standards are met within the company, to identify data protection gaps and to remedy them if necessary. A sufficiently independent and objective proof of internal compliance with GDPR requirements may be more difficult to provide by the company's own employees. However, an internal audit can be helpful to find out whether the implemented data protection measures are effective

The process of a GDPR audit

The basic process of a GDPR audit may be described as follows:

1 Setting the audit target

Companies should first define their audit target. Should a complete review of GDPR compliance take place or should it be limited to some critical company areas with particularly high data protection risks? Instead of a comprehensive audit, should only an audit of the technical and organizational security measures be carried out?

2 Audit planning

Once the audit target has been set, audit planning begins. Based on the audit target, companies may determine whether an internal or external audit is best suited to their needs. In preparation for the audit, a schedule will be drawn up to outline the timeframe and the internal responsibilities for the GDPR audit (e.g. who is the contact person for the external auditors, who is responsible for collecting the audit documents).

The core element of audit planning is the creation of the audit questionnaire that will often serve as a basis for the audit. When preparing the questionnaire, particularities of the company should be taken into consideration (for example, processing of special data categories in the company, processing of children's data). For GDPR audits, the following aspects are regularly included in the questionnaire:

- Details about the company (e.g. sector, object of the company, organization chart, number of employees)
- Data protection documentation (e.g. data protection declaration, list of processing activities, details of service providers used data processing agreements concluded)
- Internal data protection organization (e.g. existence of a data protection officer, data protection impact assessments carried out, data protection concept, handling of data subjects' rights requests, employee training)
- Information on the IT systems used (e.g. server locations, security checks carried out, access restrictions, encryption standards)

Questions are to be answered in writing and/or by submitting appropriate documents.

During the planning stage, companies should ensure that the audit will help them to find out whether the internal data protection standards are actually being applied. One way of doing this is to conduct (random) employee surveys. However, a factual investigation within the company will provide a more complete picture. For example, the audit should uncover whether employees are familiar with the internal data protection requirements, whether the data protection requirements are fully implemented and whether they are taken into account, especially in new projects. For this purpose, a factual investigation could include, for example, mock requests to exercise data subject rights or a test run for similar data protection scenarios.

The process of a GDPR audit

3 Conducting the audit

The audit is carried out by reviewing the answered questions and submitted documents for compliance with GDPR requirements. In order to evaluate the internal implementation of the GDPR obligations, a factual examination may also be carried out within the company. The actual state of the internal data protection processes is thereby put to the test.

4 Audit report and documentation

The results of the GDPR audit are summarized in an audit report. This report serves as internal documentation of the audit (audit target, scope of the audit, procedure, overview of the audited documents, audit result) and enables companies to fulfil their accountability towards the supervisory authorities.

5 Implementation of the audit recommendations

If the audit revealed a discrepancy between the actual and target status of GDPR compliance, the audit report should contain recommendations for possible measures to remedy these compliance gaps. For example, measures may be required at the legal level (e.g. revision of the declarations of consent) or at the technical/organizational level. The audited company is responsible for implementing the recommendations in order to achieve GDPR compliance.

Outlook on certification mechanisms

An external GDPR audit could be conducted with the aim of obtaining certification in accordance with Art. 42 of the GDPR. The legislator had in mind that these certifications may be presented to the supervisory authorities as sufficient proof of GDPR compliance or that they may be used to secure data transfers to third countries. On a less "official" level, such certifications could give a competitive edge to companies by proving their full GDPR compliance.

The EU Member States and supervisory authorities are primarily responsible for establishing the aforementioned certification procedures. Accredited certification bodies would be responsible for carrying out the certification procedures and for issuing certifications. However, there are no accredited certification bodies in the EU to date and therefore no corresponding certifications.

In the future, however, such procedures could make it considerably easier to prove compliance with the GDPR after undergoing a respective audit. Certifications would be beneficial in terms of compliance.

Ihre Ansprechpartner

Paul Voigt,
Lic. en Derecho

Tel +49 (0)30 88 56 36-408
p.voigt@taylorwessing.com

Highlighted as Lawyer of the year 2020
Data protection law, Best Lawyers in Germany, Handelsblatt

Next Generation Lawyer – Germany
Legal 500 Germany, 2020

TOP Lawyer for Data Protection Law
WirtschaftsWoche 2020

Wiebke Reuter

+49 30 885636-131
w.reuter@taylorwessing.com

Rita Danz

+49 30 885636-158
r.danz@taylorwessing.com

1000+ lawyers
300+ partners
28 offices
16 jurisdictions

Austria	Vienna | Klagenfurt*
Belgium	Brussels
China	Beijing* | Hong Kong | Shanghai*
Czech Republic	Brno* | Prague
France	Paris
Germany	Berlin | Düsseldorf | Frankfurt | Hamburg | Munich
Hungary	Budapest
Netherlands	Amsterdam | Eindhoven
Poland	Warsaw
Slovakia	Bratislava
South Korea	Seoul**
UAE	Dubai
Ukraine	Kyiv
United Kingdom	Cambridge | Liverpool | London | London Tech City
USA	New York* | Silicon Valley

* Representative offices ** Associated office

Europe > Middle East > Asia

taylorwessing.com