2-Control B.V.
Haagse Markt 1
4813 BA Breda
The Netherlands

+31 (0)76 50 194 70
www.2-control.nl
info@2-control.nl

Effective control of compliance level

Van: 2-Control

Datum: 2018

Betreft: GDPR compliance scan

---

1 Specific approach

Organizations have been preparing for the GDPR for more than two years. Many organizations thus enter unknown territory and go up the internet and then choose from one of the many step-by-step plans. A step-by-step plan with which you are supposedly GDPR compliant in no time. But is this step-by-step plan directly applicable to your organization?

They are often generic plans that do not help you as a unique organization. That is why it is essential to start by asking yourself the question: What is the desired compliance level?

After completing a compliance scan, you have a clear picture of the current situation and you can map out the steps to be taken in practice. This gives you an effective approach that is fully focused on your organization to become GDPR compliant.

Have you completed the GDPR implementation, but do you want to know if you are actually compliant with the new privacy legislation? Then the GDPR offers a compliance scan as a useful handle.

2 General Data Protection Regulation (GDPR)

Rules for privacy protection were established in 1995 on the basis of “EU Directives 95/46”. The “Personal Data Protection Act” (“Wet bescherming persoonsgegevens” in Dutch) was replaced in 2001, of which further guidelines were developed in 2016 regarding the obligation to report data leaks (Wbp Article 34a).

New privacy rules were adopted at European level in May 2016 through the “EU Data Protection Regulation 2016/679”. After an implementation period of 2 years, these new rules were activated from 25 May 2018 to replace the Wbp. In the Netherlands, this new law is known as the “Algemene Verordening Gegevensbescherming” (AVG) or “General Data Protection Regulation” (GDPR) international.

2.1 Need for new legislation

It is the responsibility of everyone to protect privacy and thereby ensure that personal data is always adequately protected against unauthorized processing. According to the definition of the GDPR, processing also includes viewing data.

The GDPR obliges organizations to take technical and organizational measures to guarantee this privacy. These measures result from rules for “rights for the data subject” on the one hand and “obligations for the controller and processor” on the other hand. This applies to all private and public organizations that process personal data or to whom the processing is outsourced.

3 Practical approach with useful results

2-Control is an organization with IT auditors with specializations in compliance issues and Microsoft Dynamics NAV. We support organizations with the introduction of GDPR and ensure an understandable and organization-specific approach. We always strive for a pragmatic approach with quick and useful results.

4 GDPR Compliance Scan

4.1 Objective

The objective of the 2-Control GDPR compliance scan is to provide you with insight into the compliance level of your organization for the GDPR. Based on concrete findings and recommendations, you can use the scan as a baseline measurement or as a starting point for the implementation of GDPR within your organization.

The scan is aimed at determining measures to be taken for your organization with regard to:

1. the rights of the data subject
2. the obligations of the controller and processor

It is important that you have insight into the collections of personal data within your organization. If this is not known at the start of the scan, we can help you make it clear.

4.2 Approach and result

A good scan is according the proven approach below:

1. Interview (s) with relevant stakeholders, responsible for:
    a. Information security policy;
    b. HR policy;
    c. Automation;
2. Analyzing:
    a. Personal data collections;
    b. Automation environment;
    c. Documentation;
3. Interpretation and analysis of findings;
4. Compilation of compliance status reporting with recommendations regarding:
    a. Organization;
    b. Policy (including processes and procedures);
    c. Technic;
5. Discuss findings and recommendations.

5 Support 2-Control

We are here to help you implement the GDPR correctly. The time required for a GDPR compliance scan strongly depends on the size of your company. For an average SME, our commitment varies from 1 to 3 days.

If you should have any questions regarding the execution of the GDPR compliance scan, you can ask them via our contact form.