Bavarian State Office for

data protection supervision

Ansbach, November 7, 2018

press release

Data protection checks at Bavarian companies and doctors according to the GDPR

Almost half a year after the General Data Protection Regulation (GDPR) came into force the Bavarian State Office for Data Protection Supervision (BayLDA) has its testing activities resumed and new comprehensive data protection controls in Bavaria initiated. The current tests focus on the safe operation of Online shops, protection against encryption Trojans in medical practices, compliance with the Accountability in large corporations and medium-sized companies as well as the Implementation of the information requirements in the application process.

Transition to GDPR

As the supervisory authority, the BayLDA is responsible for monitoring compliance with data protection requirements in the non-responsible for the public sector in Bavaria. This means that targeted tests are used to regularly determine must, to what extent the legal requirements for companies, clubs and associations as well as freelancers - referred to as "responsible person" under the GDPR - is actually taken into account. In previous years it had BayLDA has already carried out numerous data protection checks. With personal on-site checks of individual companies be, automated online audits at thousands of companies and large-scale written audits with multiple pages Questionnaires have so far covered a wide range of tests.

Due to the transition to the DS-GVO, the BayLDA this year focused on the innovations in the regulation informed, so that ambiguities can be eliminated as quickly as possible and those responsible can find out what is happening in the immediately changed for you to the previous data protection law. With the GDPR tests that have now started, the

Those responsible have to prove to the BayLDA that they know and comply with the new requirements. The goal is all

However, not to overwhelm small companies with data protection controls, but larger and risky organizations

tion with regard to possible sources of danger and to work towards the fact that personal

data is protected effectively and appropriately there. As a follow-up to the written exams

selected companies were also visited on site and the information provided was checked for accuracy.

Below are the exams that have recently started.

Check 1: Secure operation of online shops (cyber security)

Due to the very high risk situation on the Internet, the BayLDA continues to rely on preventive measures

Cyber security for Bavarian controllers, so that personal data from them is appropriate and effective

be protected from the daily dangers of the digital age. For this purpose, the BayLDA conducts

address

Bavarian State Office for Data Protection Supervision

boardwalk 27

91522 Ansbach

Telephone +49 (0) 981 53 1300

Fax +49 (0) 981 53 98 1300

e-mail

Website www.lda.bayern.de

presse@lda.bayern.de

Public transportation

Schlossplatz bus stops

or train station of the city and

regional lines

comprehensive automated checks to identify security gaps and in particular the operators of

Raising awareness of web applications in Bavaria. Even if the preventive nature of the online exams of the

BayLDA is highlighted, the GDPR, in addition to the existing legal obligation,

to ensure an adequate level of security when handling personal data, including in principle the

Possibility of fines against the responsible website operator in the event of violations of the "security of processing"

operator to impose.

The focus of the current cyber security control is the use of online shops. Twenty Bavarian

Online shops, randomly selected from all industries, were evaluated in terms of using outdated and

insecure eCommerce systems checked. The companies have received a detailed test letter and are

called upon to remedy identified deficiencies. The background to this test is that the BayLDA in the past

Hacking incidents of online shops have been reported for months, with attackers mostly being successful

tried to "read" the customer's payment data and later misused it for third-party transactions. So that

does not happen, website operators must regularly update (patch management) security

Import updates in order to close existing gaps in a timely manner.

Test 2: Encryption Trojans in medical practices (cyber security)

Encryption trojans (“ransomware”) are still active in Bavaria: The malware causes the

Blocked access to data and then demanded a ransom to restore the data to its original state

receive. This is achieved by reports of an infestation on the workplace computers of those responsible in Bavaria

BayLDA weekly. In the event of an infection, the malware may spread throughout the network

of the affected organization. Without data security (backups) it is only possible in a few cases to restore

the data can be created effortlessly. In most cases, however, infected companies have major problems closing again

return to a regular working day. For this reason, regular data backups and the

Raising employee awareness of valuable preventive measures.

According to the reports received by the BayLDA, doctors and smaller companies that are either

were not aware of the risk or only had inadequate security measures. The BayLDA

has therefore decided to control doctors on how to deal with and prevent ransomware attacks. target

This data protection check is to ensure suitable and effective backup behavior among doctors so that

patient data are adequately protected from the real danger of such cryptotrojans.

Test 3: Accountability in large corporations

Whether companies actually implement relevant data protection requirements in practice is not for the BayLDA always easily recognizable - at least if no on-site inspection takes place. Due to the DS-GVO, this situation has tion changed and resulted in a kind of “reversal of the burden of proof”: the supervisory authority no longer has to detect violations at the company, but the audited company must prove that it meets the requirements of the GDPR (“accountability”).

The BayLDA asked three large corporations 50 questions each and used it to check whether the respective organization had a data protection-compliant processing of personal data takes place and with data subject rights and data breaches are handled properly. The aim of this test is therefore also to determine the extent to which large Companies are able to prove compliance with the legal requirements of the GDPR. To After evaluating the responses, each of the companies contacted is subjected to an on-site inspection.

Test 4: Fulfillment of the information requirements in the application process

As early as 2015, the BayLDA carried out a major audit to check whether companies were using applicant data is handled appropriately. Some deficiencies were found in the process, which were only were lifted. With this experience, the BayLDA decided in October 2018 to again to examine the processing of personal data in application procedures.

The focus this time is to what extent the obligation to provide information to applicants is correctly implemented and Applicants ultimately also find out how their data is handled. There are currently 15 people responsible for this in Bavaria, only larger companies and clubs.

Examination 5: Implementation of the GDPR in small and medium-sized enterprises (SMEs)

The question of the status of the implementation of the GDPR also arises for small and medium-sized companies. In an examination of the general data protection organization, 20 questions have to be answered and some documents increase A focus of the control is the consideration of the risk-oriented approach of the DS-GVO, which in principle means that technical and organizational protective measures according to the risk but also to be selected according to the size and type of company. The 15 audited companies (each with over 100

employees) was selected according to the following criteria: Half of them have already complained to the BayLDA

favor. Otherwise, those responsible from different sectors from all over Bavaria were taken into account.

Outlook on pending controls: sub-service provider use and deletion of SAP systems

The BayLDA will start further tests in the next few weeks. So there are already two new controls in the

Starting blocks: On the one hand, large, internationally active companies should be checked to see whether they can

Selection of service providers that comply with data protection regulations and in particular in the event of data protection

violations

have established existing reporting processes. On the other hand, the topic "Deleting data" will be the focus

in SAP systems, form the framework of a further test.

Thomas Kranig, President of the BayLDA, comments on the new data protection checks as follows: “We have this

year, a great deal of effort was put into recruiting those responsible from all sectors - from small craftsmen's businesses,

the club, the medium-sized company to the multi-billion dollar DAX group - comprehensively on the innovations

to advise on the GDPR. The misinformation, which unfortunately is still circulating, unsettles many Bavarians

Company. We still regularly receive absurd inquiries and individual interpretations of the new data

property rights that are far removed from what really needs to be done. Our goal is therefore now through active

Tests to show what the actual test standard is and what is expected of those responsible. So that the

effort for our authority at a time when we are still dealing with countless complaints and reports

Data breaches are overwhelmed, remains manageable, we refer as part of the checks mentioned

currently only relatively few responsible persons, but at the same time publish the test letters and the associated ones

Information sheets so that all other companies can also understand what we actually query and

can then check for themselves whether they meet the requirements.”

The BayLDA provides all information on the data protection checks mentioned with sample letters and information sheets

available on his website:

Thomas Kranig

president

www.lda.bayern.de/de/kontrollen.html