Data Protection Authority of Bavaria
for the Private Sector

Ansbach, 7 November 2018

Press release

Data protection audits at Bavarian companies and physicians according to the GDPR

Less than six months after the entry into force of the General Data Protection Regulation (GDPR), the Bavarian Data Protection Authority for the Private Sector (BayLDA) has stepped up its auditing activities again and initiated new comprehensive data protection controls in Bavaria. The focus of the current audits is on the safe operation of online shops, protection against ransomware in medical practices, the fulfilment of accountability obligations for large corporations and medium-sized companies as well as the implementation of information duties in application procedures.

Transition to the GDPR

The BayLDA is the supervisory authority responsible for monitoring compliance with data protection regulations in the private sector in Bavaria. This means that focused audits must be carried out regularly to determine the extent to which the legal requirements of companies, clubs and associations as well as freelancers – referred to as "controller" under the GDPR – are actually met. In the past years, the BayLDA had already accomplished numerous data protection examinations. With personal on-site inspections of individual companies, automated online audits of thousands of companies as well as large-scale written audits with multi-page questionnaires, a broad spectrum of tests has been covered so far.

With the transition to the GDPR, this year the BayLDA has mainly informed about the new aspects of the regulation, so that ambiguities can be removed as quickly as possible and those responsible know what has changed for them in comparison to the previous data protection law. With the GDPR audits now launched, those responsible must prove to the BayLDA that they know and comply with the new requirements. The aim, however, is not to overburden small businesses with data protection controls, but to sensitise larger organisations and those fraught with risks to possible sources of danger and to work towards ensuring that personal data are effectively and adequately protected there. Following the written examinations, selected companies are partly visited on site and the accuracy of the information provided is checked. Listed below are the audits that were started recently:

Anschrift
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach

Telefon +49 (0) 981 53 1300
Telefax +49 (0) 981 53 98 1300
E-Mail presse@lda.bayern.de
Webseite www.lda.bayern.de

Öffentliche Verkehrsmittel
Bushaltestellen Schlossplatz
oder Bahnhof der Stadt- und
Regionallinien

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

Due to the very high risk situation on the Internet, the BayLDA is continuing to focus on preventive measures to cyber security for Bavarian controllers so that personal data is adequately and effectively protected from the daily dangers of the digital age. For this purpose, the BayLDA carries out comprehensive automated tests in order to identify security holes and, in particular, to sensitise the operators of web applications in Bavaria. Even if the preventive character of the BayLDA's online audits is emphasised, the GDPR in addition to the already existing legal obligation to ensure a sufficient level of security in the handling of personal data, also fundamentally provides for the possibility of imposing fines on the responsible website operator in the event of violations of the "security of processing".

The focus of the current cyber security audit is the use of online shops. Twenty Bavarian online shops, randomly selected from all industries, were examined with regard to the use of outdated and unsafe eCommerce systems. The companies have received a detailed review letter and are called upon to remedy any shortcomings identified. The background to this audit is that the BayLDA has become aware of hacking incidents of online shops in recent months, in which attackers usually successfully attempt to "read" customer payment data and later misuse it for third-party transactions. To prevent this from happening, website operators must introduce security updates through regular updates (patch management) in order to close existing holes promptly.

Audit 2: Ransomware in medical practices (cyber security)

Ransomware is still active in Bavaria: The malware blocks access to data and then demands a ransom to restore the data to its original state. Reports about an infestation of workplace computers at Bavarian controllers reach the BayLDA weekly. In the event of an infection, the malware may spread throughout the entire network of the affected organisation. Without data backups, data can only be recovered effortlessly in a few cases. In most cases, however, infected companies still have major problems returning to a regular work routine. For this reason, regular data backups and raising employee awareness are valuable preventive measures.

According to the reports received by the BayLDA, physicians and smaller companies who were either unaware of the danger or had inadequate safety measures are often affected. The BayLDA has therefore decided to control physicians in the handling and prevention of ransomware attacks. The aim of this data protection audit is to ensure that doctors have suitable and effective backup behaviour so that patient data is adequately protected against the real danger of such ransomware.

Audit 3: Accountability for large corporations

It is not always easy for the BayLDA to determine whether companies actually implement relevant data protection requirements in practice - at least if no on-site inspection takes place. However, the GDPR has changed this situation and resulted in a kind of "burden of proof reversal": The supervisory authority no longer has to determine infringements at the company itself, but the audited company must prove that it complies with the requirements of the GDPR ("accountability").

The BayLDA has asked three large corporations 50 questions each and is thus examining whether the processing of personal data in the respective organisation complies with data protection regulations and whether rights of data subjects and data breaches are correctly dealt with. The aim of this audit is also to determine the extent to which large companies are in a position to demonstrate compliance with the legal requirements of the GDPR. Once the responses have been evaluated, each of the companies contacted is subjected to an on-site inspection.

Audit 4: Fulfilment of information obligations in application procedures

As early as 2015, the BayLDA conducted a major audit of companies to determine whether they were handling applicant data properly. Some shortcomings were found, which were only remedied in the course of the processing. Based on this experience, the BayLDA decided in October 2018 to investigate again the processing of personal data in application procedures with randomly selected controllers. The focus this time is on the extent to which the duty to inform applicants is correctly implemented and applicants ultimately learn how their data is handled. At present, 15 controllers in Bavaria, exclusively larger enterprises and associations, are examined for this.

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

Small and medium-sized enterprises are also faced with the question of the status of implementation of the GDPR. In an examination of the general data protection organisation, 20 questions have to be answered and some documents have to be submitted. One focus of monitoring is the consideration of the risk-oriented approach of the GDPR, which in principle means that technical and organisational measures must be selected to suit the risk as well as the size and type of company. The 15 audited companies (each with more than 100 employees) were selected according to the following criteria: Half of them have already attracted attention at BayLDA due to complaints. Otherwise, controllers from as many different sectors as possible from all over Bavaria were taken into account.

Outlook on upcoming audits: Sub-service provider deployment and deletion in SAP systems

The BayLDA will start further examinations in the next weeks. Two new audits are already in the starting blocks: On the one hand, large, internationally operating companies are to be checked to see whether they comply with data protection regulations when selecting service providers and, in particular, whether they have established reporting processes for data breaches. On the other hand, the topic of "erasure of data", mainly for SAP systems, will form the framework for a further audit.

Thomas Kranig, President of the BayLDA, comments on the new data protection audits as follows:

"*This year, we have invested a great deal of time and effort to counsel managers from all sectors of industry - from the small craftsman enterprise, the association, the medium-size enterprise up to the billion-dollar DAX company - in the improvements of the GDPR. All the wrong information, which unfortunately still circulates, unsettles many Bavarian companies. We still regularly receive absurd enquiries and individual interpretations on the new data protection law, which are far away from what really needs to be done. It is therefore our goal to use active audits to show what the actual testing criteria is and what is expected of those responsible. In order to keep the administrative burden on our authority manageable at a time when we continue to be overwhelmed with countless complaints and notifications of data breaches, we currently include only a relatively small number of those responsible within the framework of the audits mentioned above, but at the same time publish the audit letters and associated information sheets so that all other companies can also see what we can actually query and then check for themselves whether they meet the requirements. "*

The BayLDA provides all information on the aforementioned data protection audits with sample letters and info sheets on its website:

www.lda.bayern.de/en/audits.html

Thomas Kranig
President