Bayerisches Landesamt für
Datenschutzaufsicht

Ansbach, den 7. November 2018

# Pressemitteilung

## Datenschutzprüfungen bei bayerischen Unternehmen und Ärzten nach der DS-GVO

**Knapp ein halbes Jahr nach Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) seine Prüfaktivitäten wieder verstärkt aufgenommen und neue flächendeckende Datenschutzkontrollen in Bayern angestoßen. Im Fokus der aktuellen Prüfungen steht der sichere Betrieb von Online-Shops, der Schutz vor Verschlüsselungstrojanern in Arztpraxen, die Erfüllung der Rechenschaftspflicht bei Großkonzernen und mittelständischen Unternehmen sowie die Umsetzung der Informationspflichten in Bewerbungsverfahren.**

### Übergang zur DS-GVO

Das BayLDA ist als Aufsichtsbehörde für die Kontrolle der Einhaltung der datenschutzrechtlichen Vorgaben im nicht-öffentlichen Bereich in Bayern zuständig. Das bedeutet, dass durch gezielte Prüfungen regelmäßig festgestellt werden muss, inwieweit den gesetzlichen Vorgaben bei Unternehmen, Vereinen und Verbänden sowie freiberuflich Tätigen – nach DS-GVO „Verantwortliche" genannt – tatsächlich Rechnung getragen wird. In den vergangen Jahren hatte das BayLDA bereits zahlreiche Datenschutzprüfungen durchgeführt. Mit persönlichen Vor-Ort-Kontrollen einzelner Betriebe, automatisierten Online-Audits bei tausenden Unternehmen sowie schriftlichen Großprüfungen mit mehrseitigen Fragebögen wurde bislang ein breites Prüfspektrum abgedeckt.

Durch den Übergang zur DS-GVO hat das BayLDA dieses Jahr schwerpunktmäßig über die Neuerungen der Verordnung informiert, damit Unklarheiten möglichst rasch beseitigt werden und Verantwortliche erfahren, was sich im Vergleich zum bisherigen Datenschutzrecht für sie geändert hat. Mit den nun gestarteten DS-GVO-Prüfungen müssen die Verantwortlichen dem BayLDA nachweisen, dass sie die neuen Vorgaben kennen und erfüllen. Ziel ist es dabei allerdings nicht, kleine Betriebe mit Datenschutzkontrollen zu überfordern, sondern größere und risikobehaftete Organisationen hinsichtlich möglicher Gefährdungsquellen zu sensibilisieren und darauf hinzuwirken, dass personenbezogene Daten gerade dort wirksam und angemessen geschützt werden. Im Nachgang zu den schriftlichen Prüfungen werden ausgewählte Unternehmen zum Teil auch vor Ort besucht und die gemachten Angaben auf Richtigkeit kontrolliert. Nachfolgend werden die Prüfungen aufgelistet, die vor kurzem gestartet wurden.

### Prüfung 1: Sicherer Betrieb von Online-Shops (Cybersicherheit)

Aufgrund der sehr hohen Gefährdungslage im Internet setzt das BayLDA weiter auf präventive Maßnahmen zur Cybersicherheit für bayerische Verantwortliche, damit personenbezogene Daten von diesen angemessen und wirksam vor den täglichen Gefahren im digitalen Zeitalter geschützt werden. Das BayLDA führt für diesen Zweck flächen-

**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

deckende automatisierte Prüfungen durch, um Sicherheitslücken aufzuzeigen und insbesondere die Betreiber von Webanwendungen in Bayern zu sensibilisieren. Auch wenn der vorbeugende Charakter der Onlineprüfungen des BayLDA hervorgehoben wird, besteht durch die DS-GVO neben der bereits existierenden gesetzlichen Verpflichtung, für ein ausreichendes Sicherheitsniveau im Umgang mit personenbezogenen Daten zu sorgen, auch grundsätzlich die Möglichkeit, bei Verstößen gegen die „Sicherheit der Verarbeitung" Bußgelder gegen den verantwortlichen Website-betreiber zu verhängen.

Im Fokus der aktuellen Cybersicherheitskontrolle befindet sich der Einsatz von Online-Shops. Zwanzig bayerische Online-Shops, zufällig aus allen Branchen zusammengestellt, wurden hinsichtlich der Verwendung von veralteten und unsicheren eCommerce-Systemen geprüft. Die Unternehmen haben ein detailliertes Prüfschreiben erhalten und sind aufgerufen, festgestellte Defizite zu beheben. Hintergrund dieser Prüfung ist, dass dem BayLDA in den vergangenen Monaten immer wieder Hacking-Vorfälle von Online-Shops bekannt wurden, bei denen Angreifer meist erfolgreich versuchten, Zahlungsdaten der Kunden „mitzulesen" und später für fremde Transaktionen zu missbrauchen. Damit das nicht geschieht, müssen Websitebetreiber durch regelmäßige Aktualisierungen (Patch Management) Sicherheits-updates einspielen, um so vorhandene Lücken zeitnah zu schließen.

**Prüfung 2: Verschlüsselungstrojaner in Arztpraxen (Cybersicherheit)**

Verschlüsselungstrojaner („Ransomware") sind auch in Bayern weiterhin aktiv: Durch die Schadsoftware wird der Zugriff auf Daten gesperrt und anschließend Lösegeld gefordert, um die Daten wieder im ursprünglichen Zustand zu erhalten. Meldungen über einen Befall von Arbeitsplatzrechnern bei bayerischen Verantwortlichen erreichen das BayLDA wöchentlich. Im Falle einer Infektion kann sich die Schadsoftware unter Umständen im gesamten Netzwerk der betroffenen Organisation ausbreiten. Ohne Datensicherung (Backups) kann nur in wenigen Fällen eine Wieder-herstellung der Daten mühelos erfolgen. Meist haben infizierte Unternehmen dennoch große Probleme, wieder zu einem geregelten Arbeitsalltag zurückzukehren. Aus diesem Grund sind regelmäßige Datensicherungen und die Sensibilisierung der Mitarbeiter wertvolle Vorbeugemaßnahmen.

Betroffen sind nach den eingehenden Meldungen beim BayLDA oft Ärzte und kleinere Betriebe, die sich entweder der Gefährdungslage nicht bewusst waren oder nur über unzureichende Sicherheitsmaßnahmen verfügten. Das BayLDA hat sich deshalb entschieden, Ärzte zum Umgang und Prävention von Ransomware-Attacken zu kontrollieren. Ziel dieser Datenschutzprüfung ist es, für ein geeignetes und wirksames Backupverhalten bei Ärzten zu sorgen, damit Patientendaten vor der realen Gefahr solcher Kryptotrojaner angemessen geschützt werden.

**Prüfung 3: Rechenschaftspflicht bei Großkonzernen**

Ob Unternehmen relevante Datenschutzanforderungen in der Praxis tatsächlich umsetzen, ist für das BayLDA nicht immer leicht erkennbar – zumindest wenn keine Vor-Ort-Kontrolle stattfindet. Durch die DS-GVO hat sich diese Situa-tion jedoch verändert und eine Art „Nachweislast-Umkehr" ergeben: Die Aufsichtsbehörde muss nicht mehr selbst Verstöße beim Unternehmen feststellen, sondern das geprüfte Unternehmen muss nachweisen, dass es die Vorgaben der DS-GVO einhält („Rechenschaftspflicht").

Das BayLDA hat drei Großkonzernen jeweils 50 Fragen gestellt und prüft damit, ob in der jeweiligen Organisation eine datenschutzkonforme Verarbeitung personenbezogener Daten stattfindet und mit Betroffenenrechten sowie Daten-schutzverletzungen richtig umgegangen wird. Ziel dieser Prüfung ist es also zudem festzustellen, inwieweit große Unternehmen in der Lage sind, die Einhaltung der gesetzlichen Vorgaben aus der DS-GVO auch nachzuweisen. Nach Auswertung der Antworten wird jedes der angeschriebenen Unternehmen einer Vor-Ort-Kontrolle unterzogen.

**Prüfung 4: Erfüllung der Informationspflichten in Bewerbungsverfahren**

Bereits im Jahr 2015 hat das BayLDA in einer Großprüfung Unternehmen daraufhin kontrolliert, ob mit Bewerberdaten sachgemäß umgegangen wird. Dabei wurden einige Mängel vorgefunden, die erst im Rahmen der Aufarbeitung behoben wurden. Mit dieser Erfahrung entschied sich das BayLDA deshalb nun im Oktober 2018, erneut bei zufällig ausgewählten Verantwortlichen die Verarbeitung personenbezogener Daten in Bewerbungsverfahren zu untersuchen. Schwerpunkt ist dieses Mal, inwieweit die Informationspflicht gegenüber den Bewerbern korrekt umgesetzt wird und Bewerber letztendlich auch erfahren, wie mit ihren Daten umgegangen wird. Hierzu werden derzeit 15 Verantwortliche in Bayern, ausschließlich größere Betriebe und Vereine, geprüft.

**Prüfung 5: Umsetzung der DS-GVO bei kleinen und mittelständischen Unternehmen (KMUs)**

Auch bei kleinen und mittleren Unternehmen stellt sich die Frage nach dem Stand der Umsetzung der DS-GVO. In einer Prüfung zur allgemeinen Datenschutzorganisation sind 20 Fragen zu beantworten und zum Teil Unterlagen vorzulegen. Ein Schwerpunkt der Kontrolle stellt die Berücksichtigung des risikoorientierten Ansatzes der DS-GVO dar, der im Prinzip bedeutet, dass technische und organisatorische Schutzmaßnahmen entsprechend des Risikos aber auch nach der Größe und Art des Unternehmens auszuwählen sind. Die 15 geprüften Unternehmen (mit jeweils über 100 Mitarbeitern) wurde nach folgenden Kriterien ausgesucht: Die Hälfte ist beim BayLDA bereits durch Beschwerden aufgefallen. Ansonsten wurden Verantwortliche aus unterschiedlichen Branchen aus ganz Bayern berücksichtigt.

**Ausblick auf anstehenden Kontrollen: Sub-Dienstleister-Einsatz und Löschen bei SAP-Systemen**

Das BayLDA wird in den nächsten Wochen weitere Prüfungen beginnen. So stehen bereits zwei neue Kontrollen in den Startlöchern: Zum einen soll bei großen, international agierenden Unternehmen geprüft werden, ob diese bei der Auswahl von Dienstleistern die Datenschutzvorgaben einhalten und insbesondere auch bei Datenschutzverletzungen bestehende Meldeprozesse etabliert haben. Zum anderen wird das Thema „Löschen von Daten", schwerpunktmäßig bei SAP-Systemen, den Rahmen einer weiteren Prüfung bilden.

**Thomas Kranig**, Präsident des BayLDA, äußert sich zu den neuen Datenschutzprüfungen wie folgt: *„Wir haben dieses Jahr einen sehr hohen Aufwand betrieben, um Verantwortliche aus allen Branchen – vom kleinen Handwerkerbetrieb, dem Verein, dem mittelständischen Betrieb bis hin zum milliardenschweren DAX-Konzern – umfassend zu den Neuerungen der DS-GVO zu beraten. Die Fehlinformationen, die leider immer noch kursieren, verunsichern viele bayerische Unternehmen. Wir erhalten noch regelmäßig absurde Anfragen und individuelle Interpretationen zum neuen Datenschutzrecht, die weit weg von dem sind, was wirklich gemacht werden muss. Unser Ziel ist es daher, nun durch aktive Prüfungen aufzuzeigen, was tatsächlich Prüfmaßstab ist und von den Verantwortlichen erwartet wird. Damit der Verwaltungsaufwand für unsere Behörde in Zeiten, in denen wir nach wie vor mit unzähligen Beschwerden und Meldungen über Datenschutzverletzungen überschüttet werden, überschaubar bleibt, beziehen wir im Rahmen der genannten Prüfungen derzeit nur relativ wenige Verantwortliche ein, veröffentlichen aber gleichzeitig die Prüfschreiben und dazugehörigen Informationsblätter, damit auch alle anderen Unternehmen nachvollziehen können, was wir tatsächlich abfragen und dann selbst prüfen können, ob sie die Anforderungen erfüllen."*

Das BayLDA stellt alle Informationen zu den genannten Datenschutzprüfungen mit Musterschreiben und Infoblättern auf seiner Website zur Verfügung:

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

**Thomas Kranig**
Präsident