von Rechtsanwalt **Jan Lennart Müller**

BayLDA prüft per Fragenkatalog die Umsetzung der DSGVO von kleinen und mittleren Unternehmen

Das Bayerische Landesamt für Datenschutzaufsicht (Datenschutz-Aufsichtsbehörde für Unternehmen in Bayern) führt derzeit eine Reihe von Datenschutzkontrollen (anlassbezogene und anlasslose Datenschutzprüfungen) bei Unternehmen durch. Hierbei versendet das Bayerische Landesamt für Datenschutzaufsicht einen Fragenkatalog und fordert die angeschriebenen Unternehmen auf, die gestellten Fragen binnen gesetzter Frist zu beantworten. Wie betroffene Unternehmen reagieren können und wie Sie sich als Händler auf eine solche Prüfung vorbereiten können, erfahren Sie in unserem Beitrag.

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) führt im Rahmen seiner gesetzlichen Aufgaben regelmäßig anlassbezogene und anlasslose Datenschutzprüfungen durch. **Anlassbezogene** Prüfungen erfolgen meist aufgrund von Beschwerden oder konkreten Hinweisen auf mögliche Datenschutzverstöße durch Dritte. **Anlasslose** Prüfungen erfolgen nach pflichtgemäßem Ermessen branchenunabhängig in allen Regionen Bayerns.

Rechtlicher Hintergrund

Gemäß Art. 5 Abs. 2 DSGVO ist der datenschutzrechltich Verantwortliche verpflichtet, die Einhaltung der datenschutzrechtlichen Vorgaben nachzuweisen (sog. "Rechenschaftspflicht"). Auf der anderen Seite verfügen die Datenschutzbehörden nach Art. 58 Abs. 1 lit. a und b DSGVO über gewisse Untersuchungsbefugnisse, die es ihr gestatten, den Verantwortlichen anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind und darüber hinaus Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen.

Auf dieser gesetzlichen Basis werden die Fragebögen des BayLDA an die betroffenen Unternehmen versendet.

Beschreibung der Prüfung durch das BayLDA

Hinsichtlich der **Beschreibung** der Prüfungen zur Umsetzung der DSGVO bei kleinen und mittelständischen Unternehmen (KMUs) informiert das BayLDA wie folgt:

> *"Die DS-GVO verlangt vom Verantwortlichen, dass die Einhaltung der DS-GVO nachgewiesen wird (Art. 5 Abs. 2 DS-GVO). Diese "Rechenschaftspflicht" stellt vom Grundsatz her eine "Nachweislast-Umkehr" dar, was bedeutet, dass die Einhaltung der gesetzlichen Anforderungen der Aufsichtsbehörde bei einer Kontrolle dargestellt werden muss. Während dies bei großen Unternehmen in der Regel nur anhand einer systematischen Ausgestaltung der Geschäftsprozesse erreicht werden kann, skaliert die DS-GVO bei KMUs (Kleineren und mittelständischen Unternehmen) recht gut. Die Einhaltung der datenschutzrechtlichen Anforderungen kann deutlich weniger formal erreicht werden - viele wichtige Punkte werden im Rahmen dieser Prüfung abgefragt."*

Fragenkatalog des BayLDA

Der Fragebogen des BayLDA kann **online abgerufen** werden. Die nachstehenden datenschutzrechtlichen Fragen werden im Rahmen des Fragenkatalogs an die ausgewählten Unternehmen versendet:

"1. Ist ein Datenschutzbeauftragter bestellt und der Aufsichtsbehörde gemeldet?
2. Welche Aufgaben hat Ihr Datenschutzbeauftragter?
3. Sind, falls Sie einen Datenschutzbeauftragten haben, die letzten (zwei) Audits des Datenschutzbeauftragten vor- handen und besitzen diese eine einheitliche Prüfmethodik?
4. Gibt es bei Ihnen einen Betriebsrat?
5. Sind, sofern mehrere Standorte vorhanden sind, die anderen Niederlassungen in ein einheitliches Datenschutzkon- zept eingebunden?
6. Gibt es ein Konzept im Unternehmen, wer bezogen auf den Datenschutz für was zuständig ist (z.B. Schulung der Mitarbeiter, Meldung von Datenschutzverletzungen,...)?
7. Ist ein vollständiges Verarbeitungsverzeichnis vorhanden?
8. Gibt es bei Ihnen Verarbeitungen, die Sie auf die Rechtsgrundlage "Interessenabwägung" nach Art. 6 Abs. 1 f DS-GVO stützen? Wenn ja, sind dafür dokumentierte Begründungen vorhanden?
9. Gibt es bei Ihnen Verarbeitungen, die Sie auf die Rechtsgrundlage "Einwilligung" nach Art. 6 Abs. 1 a DS-GVO stützen?
10. Existiert ein Löschkonzept (z.B. nach DIN 66398), das auch den Umgang mit Archiven und Backups regelt?
11. Werden geeignete Security-Maßnahmen zur Sicherstellung der Verfügbarkeit, Vertraulichkeit und Integrität nach Art. 32 DS-GVO getroffen?
12. Sind die Beschäftigten zur weisungsgebundenen Verarbeitung personenbezogener Daten in ihrem Arbeitsbereich sensibilisiert und verpflichtet (Art. 29 DS-GVO)?
13. Gibt es bei Ihnen Verarbeitungstätigkeiten, für die eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO gegeben ist?
14. Ist ein dokumentierter Prozess vorhanden, wie mit Auskunftsansprüchen nach Art. 15 DS-GVO umgegangen wird?
15. Wurden die Webseite(n) seit dem 25.Mai 2018 derart überarbeitet, dass auf ihnen über die Datenverarbeitung (der Webseite) ausreichend gemäß Art. 13 DS-GVO informiert wird?
16. Ist ein Verfahren vorhanden, mit dem die Antwortzeiten auf Fristeinhaltung bezüglich der Betroffenenrechte gemäß Art. 14 bis 22 sicherstellt werden.?
17. Ist ein Verfahren vorhanden, mit dem auf Anfragen der Datenschutzaufsichtsbehörden bezüglich dort eingegangener Datenschutzbeschwerden reagiert wird?
18. Sind Schulungsunterlagen vorhanden, mit denen die Personen, die an den Prozessen zur Sicherstellung der Betroffenenrechte mitarbeiten, sachgerecht informiert werden?
19. Wie viele Datenschutzverletzungen nach Art. 33/34 DS-GVO sind bei Ihnen bekannt geworden?
20. Gibt es einen (dokumentierten) Prozess, um Datenschutzverletzungen innerhalb 72 Stunden (auch an Wochen- enden/Feiertagen) bei der zuständigen Aufsichtsbehörde zu melden?"

Wie sollten sich betroffene Unternehmen verhalten uns welche Vorsorge sollte man treffen?

Wenn Sie als Unternehmen Adressat eines solchen Fragebogens des BayLDA sind, sollten Sie diese Auskunftsanforderung unbedingt ernst nehmen! In diesem Fall sollten Sie rechtskundigen Rat einholen und sich bei der Beantwortung der gestellten Fragen ausreichend beraten lassen. Es geht in solchen Fällen auch immer darum, drohende Bußgelder im Ansatz zu vermeiden oder zumindest eine günstige Ausgangslage für die weitere Kommunikation mit der Datenschutzaufsichtsbehörde zu schaffen.

Wenn Sie Vorsorgemaßnahmen treffen möchten, dann prüfen Sie, ob Sie

- einen **Datenschutzbeauftragten** bestellen müssen (und dies noch nicht getan haben)
- Ihre Datenschutzerklärung auf dem aktuellsten Stand haben
- ein **Verarbeitungsverzeichnis** für Ihre Datenverarbeitungsvorgänge angelegt haben

Wenn Sie noch keine aktuelle DSGVO-konforme Datenschutzerklärung nutzen und/oder ein Verarbeitungsverzeichnis noch nicht erstellt haben, empfehlen wir Ihnen unsere ***Schutzpakete** mit besonderer Ausrichtung auf die Einhaltung der DSGVO-Vorgaben! Mit unseren Schutzpaketen können Sie die Themen Datenschutzerklärung und Verarbeitungsverzeichnis schnell und einfach in den Griff bekommen!

Orientierungshilfe des Bayerischen Landesbeauftragten zu den datenschutzrechtlichen Informationspflichten

Der Bayerische Landesbeauftragte für den Datenschutz hat aktuell eine lesenswerte Orientierungshilfe zu Informationspflichten nach der EU-Datenschutzgrundverordnung veröffentlicht. Sie können diese Orientierungshilfe **hier** einsehen.

Im Rahmen dieser Orientierungshilfe werden die einzelnen Informationspflichten nach Art. 13, 14 EU-Datenschutzgrundverordnung näher erläutert - zudem werden zahlreiche derzeit auch zwischen den Aufsichtsbehörden diskutierte Fragestellungen behandelt. Zwar besitzt diese Orientierungshilfe des Bayerischen Landesbeauftragten für Datenschutz keinen rechtlich verbindlichen Charakter, jedoch beinhaltet die Orientierungshilfe zahlreiche praktische Empfehlungen, welche als wertvolle Richtschnur für Unternehmen fungieren können.

Autor:
RA Jan Lennart Müller
Rechtsanwalt