Datenschutz-NEWS

DRIMALSKI &Partner

…zu den aktuellen Ereignissen der letzten Wochen [01/2022]

Anlasslose Prüfungen bei Unternehmen durch Aufsichtsbehörden

Datenschutzprüfung „Ransomware Prävention“ der Aufsichtsbehörde Bayern

Nach eigenen Angaben hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) eine neue Stabstelle „Prüfverfahren des BayLDA“ gegründet.

Diese hat am 30.11.2021 gleich mit der Arbeit begonnen und kleine und mittlere Unternehmen, kleinere Krankenhäuser, Schulen und Arztpraxen im Hinblick darauf kontrolliert, ob diese **geeignete technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO** gegen Ransomware-Angriffe getroffen haben. Das Ziel ist die **Gewährleistung eines Basisschutzes gegen Ransomware-Angriffe**. Mehr Informationen zur Prüfaktion sind auf der **BayLDA-Website**[1] zu finden.

Die Unternehmen werden nach dem Zufallsprinzip ausgewählt. Mit einem **Anschreiben**[2] wurden/werden aktuell diese ausgewählten Unternehmen im Hinblick auf das verstärkte Aufkommen von Ransomware-Angriffe informiert. Dabei erhalten sie dann einen **Antwortbogen**[3], den sie zurücksenden sollen. Dieser ist in 5 zielgerichtete Abschnitte unterteilt:

1) Systemlandschaft
2) Patch Management
3) Backup-Konzept
4) Überprüfung des Datenverkehrs
5) Awareness und Berechtigungen

Nach Angaben des BayLDA kann es **im Einzelfall auch zu Vor-Ort-Kontrollen** kommen, um die Umsetzung der angegebenen Maßnahmen zu überprüfen. Ebenso könnten Dokumentationen und andere Unterlagen zu den abgefragten Themenschwerpunkten im weiteren Prüfverlauf angefordert werden, heißt es.

Das BayLDA hat eine **Handreichung**[4] zur Beantwortung der Fragen veröffentlicht, die es den Unternehmen recht einfach ermöglichen sollte, die Fragen zu beantworten und ggf. auch schon weitere Maßnahmen zu treffen. Außerdem gibt es noch eine **allgemeine Information zum Thema Ransomware**[5] vom BayLDA.

Stellt sich die Frage: „Müssen Unternehmen diese Fragen beantworten?“ In dem Anschreiben, das auf der Website des BayLDA veröffentlicht ist, gibt es zwar eine „Aufforderung“, den Prüfbogen bis zur genannten Frist zurückzusenden. Da das Anschreiben aber anscheinend nicht mit einer Rechtsbehelfsbelehrung versehen ist und auch ansonsten keine Konsequenzen für die Nichtabgabe angedroht werden, ist fraglich, ob es sich bei dem Schreiben um einen „Verwaltungsakt“ handelt. Käme man zu dem Ergebnis, dass es sich nicht um einen Verwaltungsakt handeln würde, dann wäre eine Antwort auf das Anschreiben zunächst nicht verpflichtend.

Wie häufig ist es also ggf. auch eine taktisch-strategische Frage, ob hier geantwortet werden soll oder nicht. **Wenn ein Unternehmen im Bereich Ransomware-Schutzmaßnahmen nicht gut aufgestellt ist, sollte der Fokus darauf gesetzt werden, die Lücken im Bereich der Maßnahmen zügig zu schließen.** Vorsicht: Eine Nichtantwort kann ggf. auch dazu motivieren, dass doch einmal ein Aufsichtsbehördenmitarbeiter „an die Tür klopft“.

Quellen: ZD-Aktuell 2021 (05572); Datenschutz-Guru GmbH, Flensburg, 2021

Datenschutzprüfung „Selbstauskünfte Mietinteressent/innen“ der Aufsichtsbehörde Bayern

Das BayLDA nimmt nach eigenen Angaben – insbesondere in Ballungsgebieten – wahr, dass Mietinteressierte von Vermieterinnen und Vermietern **umfangreiche Formulare zur Selbstauskunft** erhalten, die von diesen im Vorfeld zu einer Wohnungsbesichtigung ausgefüllt werden sollen. Hier scheint es zu einer Reihe von Beschwerden oder Nachfragen von Personen gekommen sein, die entsprechende Formulare zur Selbstauskunft erhalten haben.

Es wurden bzw. werden deshalb seit dem **14.01.2022** Immobilien- und Hausverwaltungen in Bayern hierzu angeschrieben. Es ist davon auszugehen, dass es sich um Stichprobenverfahren handelt. Ziel der Aktion ist die **Prüfung der Einhaltung datenschutzrechtlicher Vorgaben bei der Mieterbewerbung**.

In dem **Anschreiben**[6] wird der Anlass für die Prüfung sowie der Ablauf geschildert. Es wird insbesondere eine Frist zur Beantwortung gesetzt.

---

[1] Abgerufen am 03.02.2022: https://www.lda.bayern.de/de/kontrollen_stabsstelle.html
[2] Abgerufen am 03.02.2022: https://www.lda.bayern.de/media/pruefungen/Ransomware_Praevention_Anschreiben.pdf
[3] Abgerufen am 03.02.2022: https://www.lda.bayern.de/media/pruefungen/Ransomware_Praevention_Antwortbogen.pdf
[4] Abgerufen am 03.02.2022: https://www.lda.bayern.de/media/pruefungen/Ransomware_Praevention_Handreichung.pdf
[5] Abgerufen am 03.02.2022: https://www.lda.bayern.de/media/pruefungen/Ransomware_Praevention_Infoblatt.pdf
[6] Abgerufen am 03.02.2022: https://www.lda.bayern.de/media/pruefungen/Selbstauskuenfte_Anschreiben.pdf

Es ist dann von den Haus- und Immobilienverwaltungen ein **Antwortbogen**[7] („Prüfbogen“) auszufüllen und zurückzusenden. Dieser beinhaltet Fragen zu diesen Themen:

1) Kommt ein Formular zur **Selbstauskunft** bei Mietinteressierten zum Einsatz?
2) Einzelne **Fragestellungen** zu bestimmten Angaben in der Selbstauskunft
3) Auf welche **Rechtsgrundlage** wird die Datenverarbeitung gestützt?
4) **Aufbewahrungsdauer** der Daten
5) Das „Ob“ und „Wie“ einer **Information** der Mietinteressierten zur Datenverarbeitung (Art. 13 DSGVO)

Zusätzlich gibt es ein **Informationsblatt**[8] zur Prüfung der Selbstauskunft von Mietinteressentinnen/Mietinteressenten.

Stellt sich die Frage: „Müssen Unternehmen diese Fragen beantworten?“ Es ist zu empfehlen, den Fragebogen entsprechend auszufüllen und zurückzusenden (ausgenommen Fälle, in denen man sich damit offensichtlich selbst belasten würde). Die Aufsichtsbehörde recht eindeutige Hinweise dazu, in welchem Umfang sie die Datenverarbeitung im Zusammenhang mit Selbstauskünften für Mietinteressierte für zulässig hält. Insoweit verweist sie u.a. auf folgende Informationen: DSK-Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressentinnen“[9] und FAQ des BayLDA[10].

Quelle: Datenschutz-Guru GmbH, Flensburg, 2022

Datenschutzprüfung „Rechtswidriges Tracking auf Webseiten“ der Aufsichtsbehörde Berlin

Angesichts der andauernden Defizite beim Einsatz von Tracking-Techniken und Drittdiensten auf Webseiten hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) eine großangelegte Aktion am 09.08.2021 gestartet. **Rund 50 Berliner Unternehmen erhielten postalisch die Aufforderung, das Tracking auf ihren Webseiten in Einklang mit den geltenden Datenschutzregeln zu bringen.** Andernfalls wird die Aufsichtsbehörde förmliche Prüfverfahren einleiten, die zu einer Anordnung oder einem Bußgeld führen können. Auch wenn viele Webseiten mittlerweile differenzierte Cookie-Banner mit mehreren Ebenen anzeigen, wird hiermit häufig gar keine wirksame Einwilligung eingeholt. Die damalige BlnBDI Maja Smoltczyk teilte mit:

> *„Die Rechtslage ist eindeutig: Wenn Webseiten-Betreibende das Verhalten ihrer Nutzer*innen mit Hilfe von Cookies und anderen Technologien verfolgen wollen, benötigen sie dafür eine Rechtsgrundlage. […] Aus dem Datenschutzrecht ergibt sich, dass es ebenso einfach sein muss, Tracking abzulehnen, wie darin einzuwilligen. Die Ablehnung darf nicht aufwendiger oder gar versteckt sein. […] Zudem werden die Einwilligungsabfragen gerne eingebettet in unvollständige oder missverständliche Angaben und Beschriftungen. Wie die Webseitenbetreibenden bei solch einer Gestaltung nachweisen wollen, dass die Nutzer*innen freiwillig und informiert zugestimmt haben, ist mir ein Rätsel.“*

Für ihre Aktion hat die Aufsichtsbehörde die Gestaltungsmerkmale und konkreten Datenströme auf den ausgewählten Webseiten dokumentiert und die Betreibenden **mit den konkreten datenschutzrechtlichen Defiziten konfrontiert**. In ihren Schreiben setzt sie die dokumentierten Sachverhalte in Relation zu den rechtlichen Bestimmungen und weist auf besonders kritische Punkte im Einzelfall hin. Neben den oben genannten Mängeln stellt es auch ein anhaltendes und großes Problem dar, in welchem Ausmaß **Tracking auf andere Rechtsgrundlagen als auf eine Einwilligung** gestützt wird, ohne dass die gesetzlichen Anforderungen hierfür erfüllt sind.

Die Hinweisschreiben wurden an Unternehmen gesendet, deren Cookie-Banner als besonders mangelhaft aufgefallen sind, die vergleichsweise viele Nutzer*innen haben oder die möglicherweise besonders sensitive Daten verarbeiten. Betroffen sind Unternehmen aus diversen Branchen, insbesondere Online-Handel, Immobilien, Finanzen, Soziale Netzwerke, Recht-Dienstleistungen, Software, Gesundheit, Bildung und Vergleichsportale. **Die Verantwortlichen wurden aufgefordert, die Datenverarbeitung unverzüglich in Einklang mit den datenschutzrechtlichen Vorgaben zu bringen.** In jedem Fall erfolgt eine zweite Dokumentation der Webseiten, die je nachdem, ob vergangene und/oder andauernde Verstöße festgestellt werden, weitere Maßnahmen der Behörde nach sich ziehen kann.

Quelle: Pressemitteilung des BlnBDI, Berlin, 2021

Eine erste Reaktionen auf eine unwirksame Einwilligung hat die belgische Datenschutzbehörde „BE DPA“ dazu veranlasst, gegenüber der IAB Europe (Verband für das digitale Marketing-/Werbeökosystem) ein Bußgeld in Höhe von 250.000 € auszusprechen.[11]

[7] Abgerufen am 03.02.2022: https://www.lda.bayern.de/media/pruefungen/Selbstauskuenfte_Antwortbogen.pdf
[8] Abgerufen am 03.02.2022: https://www.lda.bayern.de/media/pruefungen/Selbstauskuenfte_Infoblatt.pdf
[9] Abgerufen am 03.02.2022: https://www.datenschutzkonferenz-online.de/media/oh/20180207_oh_mietauskuenfte.pdf
[10] Abgerufen am 03.02.2022: https://www.lda.bayern.de/de/faq.html
[11] Abgerufen am 03.02.2022: https://www.dataprotectionauthority.be/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr