Verwaltungsgemeinschaft Margetshöchheim
Herr Horn
Mainstr. 15
97276 Margetshöchheim

Verwaltungsgemeinschaft Margetshöchheim

25.09.2018, 9.00 bis 11.45 Uhr

Gesprächsteilnehmer der Verwaltungsgemeinschaft: Herr Horn (Geschäftsleiter, Datenschutzbeauftragter), Frau Langhirt (Systembetreuung)

GKDS: Herr Mattern

A. Datenschutzstruktur

Gibt es eine Datenschutz-Geschäftsordnung?

Ist darin die datenschutzrechtliche Verantwortung und Zuständigkeit beschrieben?

Ist darin die Ablauforganisation (z.B. Information der Beschäftigten, Beteiligung des behördlichen DSB, Verfahren bei Datenschutzverletzungen) beschrieben?

Ist ein Datenschutzbeauftragter benannt?

An die Verwaltungsgemeinschaft angeschlossen ist ein Jugendzentrum. Bei der Umsetzung der DSGVO ist dieses auch mit einzubeziehen.

Eine Dienstanweisung zum Thema Datenschutz wurde erstellt aber noch nicht verabschiedet.

Der Geschäftsleiter ist als Datenschutzbeauftragter bestellt. Diese Kombination (Geschäftsleiter – DSB) ist jedoch nicht möglich, da es regelmäßig zu Interessenskonflikten kommen wird. Auch die Aufsicht wird dies nicht tolerieren.

Empfehlungen: Die an die Verwaltungsgemeinschaft angeschlossene Einheit (Jugendzentrum) ist bei der Umsetzung der DSGVO zu berücksichtigen. Die vorbereitete Dienstanweisung zu datenschutzrechtlichen Themen sollte überprüft, ggf. ergänzt und verabschiedet werden. Die Kenntnisnahme durch die Mitarbeiter ist zu dokumentieren. Für das Amt des Datenschutzbeauftragten ist eine andere Lösung anzustreben. Die GKDS kann einen behördlichen Datenschutzbeauftragten in seiner Arbeit beratend unterstützen oder einen externen Datenschutzbeauftragten stellen.

B. Verzeichnis der Verarbeitungstätigkeiten und Datenschutz-Folgenabschätzung

Gibt es ein aktuelles Verzeichnis der Verarbeitungstätigkeiten?
Anmerkung: Wird für AKDB Verfahren vollständig ausgefüllt bereitgestellt und gepflegt.

Ist ein Verfahren eingerichtet, das klärt, ob eine Datenschutz-Folgenabschätzung durchzuführen ist?

Werden bei der Durchführung einer Datenschutz-Folgenabschätzung die Risiken und geplante Abhilfemaßnahmen berücksichtigt?
Anmerkung: Für AKDB Verfahren wird eine Risikoanalyse und falls notwendig eine Datenschutz-Folgenabschätzung geliefert. Sofern die Einsatzvoraussetzungen vorliegen, können diese verwendet werden.

Ist sichergestellt, dass der DSB bei der Datenschutz-Folgenabschätzung zu Rate gezogen wird?

Das Verzeichnis der Verarbeitungstätigkeiten wurde erstellt. Die einzelnen Verarbeitungstätigkeiten sind noch nicht beschrieben.

Verfahren zur Risikobetrachtung und zur Dokumentation, ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss, sind nicht vorhanden.

Empfehlung: Die einzelnen Verarbeitungstätigkeiten sind vollständig zu beschreiben. Daran anschließend kann die Risikoanalyse zur Datenschutz-Folgenabschätzung dokumentiert werden. Die einzelnen Dokumente sollten zentral verwaltet werden.

C. Umsetzung der Betroffenenrechte

Sind die Informationspflichten bei Datenerhebung umgesetzt?
Anmerkung: Für AKDB Verfahren gibt es Infoblätter.

Sind die Datenschutzhinweise auf der Webseite umfassend und aktuell?

Ist ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zeitnah (innerhalb eines Monats) und vollständig beantworten zu können?

Sind Verfahren eingerichtet, die eine unverzügliche Berichtigung oder Löschung von Daten gewährleisten?

Die Informationspflichten sind noch nicht vollständig umgesetzt. Bislang ist ein Aushang zum Pass- und Meldewesen vorhanden. Bei einer Datenerhebung (z.B. mit Hilfe von Formularen) ist keine systematische Information gewährleistet.

Der Datenschutzhinweis auf der Webseite wurde bereits angepasst. Es ist jedoch noch nicht sichergestellt, dass er den Anforderungen der DSGVO entspricht.

Es sind keine Prozesse eingerichtet, die gewährleisten, dass ein Antrag auf Auskunft, Berichtigung oder Löschung zeitnah und innerhalb der gegebenen Frist bearbeitet werden kann.

Empfehlung: Die Informationspflichten müssen noch vollständig umgesetzt und auch dokumentiert werden. Der Datenschutzhinweis auf der Webseite ist zu überprüfen und ggf. anzupassen. Verfahren zur Bearbeitung von Auskunftsanfragen, Berichtigung oder Löschung sind einzurichten und im Rahmen der unter Punkt A erwähnten Dienstanweisung zu dokumentieren.

D. Auftragsverarbeitung

Sind externe Dienstleister in die Datenverarbeitung eingebunden?

Gibt es eine Übersicht der Auftragsverarbeiter?

Wurde mit allen Auftragsverarbeitern ein Vertrag mit dem Mindestinhalt nach Art. 28 (3) DSGVO geschlossen?
Anmerkung: Die AKDB erfüllt die Anforderungen als Auftragsverarbeiter. Angepasste Verträge zwischen der Kommune und der AKDB werden von der AKDB bereitgestellt.

Eine zentrale, vollständige Übersicht der Auftragsverarbeiter existiert nicht. Es ist derzeit nicht sichergestellt, dass mit allen externen Dienstleistern, die personenbezogene Daten verarbeiten, gesetzeskonforme Verträge geschlossen wurden.

Zu den großen Dienstleistern liegen Verträge zur Auftragsverarbeitung vor.

Empfehlung: Eine Übersicht der Auftragsverarbeiter sollte erstellt werden. Mit allen externen Dienstleistern, die personenbezogene Daten verarbeiten, sind Verträge zur Auftragsverarbeitung zu schließen.

E. Meldepflicht bei Datenschutzvorfällen

Ist sichergestellt, dass eine Meldung innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls an die Aufsichtsbehörde erfolgen kann?

Ist festgelegt, wie bei einem hohen Risiko für die Betroffenen eine Benachrichtigung dieser Personen stattfindet?

Ist festgelegt, wer mit der Aufsichtsbehörde kommuniziert?

Bislang sind keine Prozesse eingerichtet und beschrieben, die eine Erkennung und Meldung von Datenschutzvorfällen sicherstellen. Es sind nicht alle Mitarbeiter darüber informiert, dass bei Auftreten eines solchen Vorfalls akuter Handlungsbedarf besteht.

Es ist noch nicht festgelegt, wie eine eventuell notwendige Benachrichtigung von betroffenen Personen stattfindet und wer mit der zuständigen Aufsichtsbehörde kommuniziert.

Empfehlung: Es muss ein Prozess eingerichtet werden, der festlegt, wie eine Meldung an die Aufsichtsbehörde unter Einhaltung der Frist sichergestellt werden kann, wer mit der Aufsichtsbehörde kommuniziert und wie eine Benachrichtigung von betroffenen Personen stattfindet. Dieser Prozess ist im Rahmen der unter Punkt A erwähnten Dienstanweisung zu dokumentieren.

F. Dokumentations- und Rechenschaftspflichten

Kann die Einhaltung von datenschutzrechtlichen Vorschriften durch die verantwortliche Stelle nachgewiesen werden? Insbesondere betrifft dies: Einwilligung, Auskunftsansprüche, Auftragsverarbeitung, Verzeichnis von Verarbeitungstätigkeiten, Datenschutzvorfälle.

Derzeit kann die Verwaltungsgemeinschaft die Einhaltung der datenschutzrechtlichen Vorschriften nicht durch eine geeignete Dokumentation nachweisen.

Es ist kein System vorhanden, in dem alle Informationen und Dokumente zusammenlaufen und verwaltet werden.

Empfehlung: Es ist ein zentrales System einzurichten, in dem die Datenschutzaktivitäten und die dazugehörigen Dokumente organisiert und dokumentiert werden.

G. Schulung und Sensibilisierung der Mitarbeiter

Gibt es ein Konzept zur erstmaligen und auffrischenden Schulung/Sensibilisierung der Mitarbeiter?

Werden die Mitarbeiter zur Einhaltung des Datenschutzes verpflichtet?

Eine Schulung bzw. Sensibilisierung zum Datenschutz wurde bisher nicht vorgenommen. Für eine laufende Auffrischung und Aktualisierung der Kenntnisse gibt es kein Konzept.

Die Mitarbeiter haben eine separate Verpflichtung zur Einhaltung des Datenschutzes unterschrieben.

Empfehlung: Durch die Einführung eines Schulungskonzepts ist sicherzustellen, dass die Mitarbeiter regelmäßig über datenschutzrechtlich relevante Themen informiert werden. Insbesondere ist dies auch bei neuen Mitarbeitern wichtig. Es muss nachgewiesen werden können, dass die Mitarbeiter an Schulungen teilgenommen haben bzw. dass eine Sensibilisierung stattgefunden hat.

H. Informations-Sicherheits-Management-System

Sind technische und organisatorische Maßnahmen umgesetzt, um sicherzustellen und den Nachweis erbringen zu können, dass die Verarbeitung personenbezogener Daten gemäß der DSGVO erfolgt? Werden diese Maßnahmen überprüft und ggf. aktualisiert?

Wurden technische und organisatorische Maßnahmen getroffen, die darauf ausgelegt sind, die Datenschutzgrundsätze (z.B. Datenminimierung) wirksam umzusetzen?

Sind Voreinstellungen eingerichtet, so dass nur personenbezogene Daten die für den jeweiligen Verarbeitungszweck erforderlich sind, verarbeitet werden? Dies gilt für Menge, Umfang, Speicherfrist und Zugänglichkeit.

Wurden technische und organisatorische Maßnahmen getroffen, die die Sicherheit der Datenverarbeitung (Pseudonymisierung, Verschlüsselung, Wiederherstellbarkeit, Vertraulichkeit/Integrität/ Verfügbarkeit/Belastbarkeit der Systeme, regelmäßige Überprüfung der Maßnahmen) gewährleisten? Wurden dabei insbesondere die Risiken angemessen berücksichtigt?

Entsprechen die Schutzmaßnahmen dem aktuellen Stand der Technik?

Derzeit läuft kein Projekt zur Einführung eines Informations-Sicherheits-Management-Systems. Der Zeitpunkt der Umsetzung ist noch offen.

Empfehlung: Das Projekt sollte begonnen werden. Im Rahmen des Datenschutzes kann dann darauf verwiesen werden. Somit werden hier Synergien genutzt und Doppelarbeiten vermieden.

I. Videoüberwachung

Sind die inhaltlichen Voraussetzungen (Wahrung berechtigter Interessen, Erforderlichkeit, Interessenabwägung) ausreichend berücksichtigt?

Sind die Transparenz- und Informationspflichten beachtet (Piktogramm, Verantwortlicher mit Kontaktdaten, DSB, Verarbeitungszwecke und Rechtsgrundlagen, Angabe des berechtigten Interesses, Speicherdauer, Hinweis auf weitere Betroffenenrechte)?

Sind diese Informationen am Ort der Videoüberwachung zugänglich (z.B. Aushang)?

Ist die Speicherdauer (i.d.R. 48 Stunden) festgelegt und wird das Löschungsgebot beachtet?

Ist das eingesetzte System sicher und datenschutzfreundlich gestaltet?

Die Verwaltungsgemeinschaft betreibt als verantwortliche Stelle keine Anlagen zur Videoüberwachung.

J. Zusammenfassung

Die an die Verwaltungsgemeinschaft angeschlossene Einheit (Jugendzentrum) ist bei der Umsetzung der DSGVO zu berücksichtigen. Die vorbereitete Dienstanweisung zu datenschutzrechtlichen Themen sollte überprüft, ggf. ergänzt und verabschiedet werden.

Für das Amt des Datenschutzbeauftragten ist eine andere Lösung anzustreben.

Die einzelnen Verarbeitungstätigkeiten sind vollständig zu beschreiben. Daran anschließend kann die Risikoanalyse zur Datenschutz-Folgenabschätzung dokumentiert werden. Die einzelnen Dokumente sollten zentral verwaltet werden.

Die Informationspflichten müssen noch vollständig umgesetzt und auch dokumentiert werden. Der Datenschutzhinweis auf der Webseite ist zu überprüfen und ggf. anzupassen. Verfahren zur Bearbeitung von Auskunftsanfragen, Berichtigung oder Löschung sind einzurichten und im Rahmen der Dienstanweisung zu dokumentieren.

Eine vollständige Übersicht der Auftragsverarbeiter muss erstellt werden. Es ist zu prüfen, ob mit den externen Dienstleistern gesetzeskonforme Verträge zur Auftragsverarbeitung existieren. Falls nicht, sind entsprechende Verträge zu schließen.

Bezüglich der Meldung von Datenschutzvorfällen an die Aufsichtsbehörde ist ein Prozess einzurichten, der festlegt, wie eine Meldung an die Aufsichtsbehörde unter Einhaltung der Frist sichergestellt werden kann, wer mit der Aufsichtsbehörde kommuniziert und wie eine Benachrichtigung von betroffenen Personen stattfindet. Dieser Prozess ist im Rahmen der Dienstanweisung zu dokumentieren.

Es ist ein zentrales System einzurichten, in dem die Datenschutzaktivitäten und die dazugehörigen Dokumente organisiert und dokumentiert werden.

Durch die Einführung eines Schulungskonzepts ist sicherzustellen, dass die Mitarbeiter regelmäßig über datenschutzrechtlich relevante Themen informiert werden. Es muss nachgewiesen werden können, dass die Mitarbeiter an Schulungen teilgenommen haben bzw. dass eine Sensibilisierung stattgefunden hat.

Ein Projekt zur Einführung eines Informations-Sicherheits-Management-Systems sollte zügig begonnen werden, um Synergien zu nutzen.

Zusammenfassend kann gesagt werden, dass die Vorgaben der DSGVO zu einem sehr großen Teil noch nicht umgesetzt worden sind.

K. Angebot der GKDS

Die GKDS unterstützt Sie gerne bei der weiteren Umsetzung der Vorgaben der DSGVO und erstellt Ihnen ein auf der Bestandsaufnahme basierendes Angebot.

Die GKDS bietet an, einen externen Datenschutzbeauftragten zu stellen oder den behördlichen Datenschutzbeauftragten bei seiner Arbeit zu begleiten.

_____

Rainer Mattern
Zertifizierter Datenschutzbeauftragter (TÜV Süd)
Externer Mitarbeiter der GKDS