

AUCH FÜR PORTALE: DATENSCHUTZ AUS EINER HAND GUT GERÜSTET ZUM E-GOVERNMENT

Kaum eine Stelle nutzt so viele personenbezogene Daten wie die öffentliche Verwaltung. Das Eintrittstor für die digitale Verarbeitung dieser Daten sind Portale wie OpenR@thaus oder Portalverbünde wie OpenKreishaus. Zur Erfüllung der damit verbundenen umfangreichen Anforderungen der DSGVO profitieren ITEBO-Kunden von zahlreichen, exakt auf den kommunalen Alltag zugeschnittenen Dienstleistungen. Diese umfassen Beratungs- und Schulungsangebote sowie umfangreiche datenschutzbezogene Services, wie zum Beispiel einen riesigen Pool an Checklisten, Vertragsmustern, Verarbeitungsverzeichnis und Vorlagen bis hin zur Stellung eines Datenschutzbeauftragten.

DIE DATENHOHEIT DER BÜRGERKONTEN

Das Anlegen eines Bürgerkontos in OpenR@thaus erfordert die einmalige Registrierung durch den Bürger. Erhoben und verarbeitet werden die erforderlichen Daten, um das Anliegen der Bürger und Bürgerinnen erfüllen zu können. Die Hoheit über den angelegten Account liegt beim Bürger selbst, auch kann das Konto jederzeit wieder gelöscht werden. Für die Rechtmäßigkeit der Nutzung der Daten bzw. die dazugehörigen Informationsobliegenheiten stehen jedoch die Kommunen in der Verantwortung. „OpenR@thaus stellt eine allgemeine Datenschutzerklärung bereit. Diese wird auf den Webseiten von OpenR@thaus verlinkt und ist unmittelbar von jeder (Sub-)Seite aus erreichbar. Für die nutzende Verwaltung sind lediglich wenige Anpassungen erforderlich, bei deren Analyse und Erstellung wir unsere Kunden detailliert unterstützen“, erläutert Klaus Exner aus dem Servicebereich Datenschutz und IT-Sicherheit der ITEBO.

VERSCHLUNGEN: PORTALE UND PORTALVERBÜNDE

- Wichtig ist es, in einem ersten Schritt zu klären, wer Daten erhebt, wer sie nutzt und wo Daten letztendlich gehostet werden. Denn gerade Portalverbünde

mit ihren integrierten Fachverfahren und Prozessen fordern den Datenschutz in hohem Maße, da digitale Identitäten und Daten den Raum einer einzelnen Verwaltung verlassen und gemeindeübergreifend zur Verfügung stehen. „Wir gehen derzeit mit verschiedenen Szenarien in Bezug auf die Nutzung von Daten in OpenR@thaus bzw. OpenKreishaus um. Entweder wird OpenR@thaus von einer Kommune allein genutzt, somit liegen Erhebung und Nutzung der Daten für die jeweilig angeschlossenen Prozesse bei der Kommune. In den Portalverbünden betreibt jedoch der Landkreis das OpenKreishaus und stellt den Kommunen die Lizenzen für OpenR@thaus zur Verfügung. In diesem Szenario teilt sich die Datenverantwortung: Alle Kontodaten liegen beim Landkreis, alle antragsbezogenen Daten bei der jeweiligen Kommune. Im dritten Fall agiert der Landkreis sowohl als Datenverantwortlicher für die angeschlossenen Kommunen, bietet darüber hinaus in einem Open R@thaus seine eigenen Dienstleistungen für Bürger und Bürgerinnen“, berichtet Dörte Wilhelms aus dem Servicebereich E-Services und DMS der ITEBO.

KLARE VERTEILUNG VON ROLLEN UND AUFGABEN

Verantwortlich für die Einhaltung der DSGVO ist immer die datenerhebende Institution. Doch übernimmt eine öffentliche Verwaltung oder ein IT-Unternehmen eine Leistung für einen öffentlichen Auftraggeber, ist ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO notwendig. Konkret: Für die Lieferung, Wartung und Installation der Portallösung, aber auch für den Betrieb der Datenbanken im Rechenzentrum müssen Auftraggeber wie Kommunen oder Landkreise mit der ITEBO eine Vereinbarung zur Auftragsverarbeitung abschließen. Liegen die Konto-Daten eines Portalverbundes bei einem Landkreis, benötigt dieser einen Vertrag für das Prozedere der Auftragsdatenverarbeitung mit den beteiligten Kommunen. Dieser kann, so die derzeitige Einschätzung, nach Art. 28 DSGVO abgebildet werden. Klaus Exner weiß aus der täglichen Praxis: „Der Umgang mit der Umsetzung der komplizierten DSGVO-Anforderungen ist für viele

Verwaltungen in Bezug auf die Portale und Portalverbünde noch Neuland. Deshalb unterstützen wir bei der organisatorischen Klärung und der Erstellung der Vertragswerke.“

DIE KRUX MIT DEN PROZESSUALEN DETAILS

Auch für Fachverfahren und alle Prozesse, die in OpenR@thaus integriert werden, gilt: Sie verarbeiten Daten. Welche Daten für die jeweiligen Prozesse erforderlich sind und verarbeitet werden dürfen, regeln die unterschiedlichsten Gesetze wie z.B. das Bundesmeldegesetz, das niedersächsische Gesetz über das Halten von Hunden oder auch die Gewerbeordnung. Wann und wie Daten erhoben, abgespeichert und verarbeitet werden und welchen Vorgaben die Übermittlung dieser Daten unterliegt, regelt u.a. das NDSG. Doch die Einhaltung von Transparenz und die Erfüllung der umfassenden Aufklärungs- und Informationspflichten der DSGVO obliegt den anbietenden Kommunen.

Da Bürger und Bürgerinnen wissen möchten, auf welche Art, in welchem Umfang und zu welchem Zweck personenbezogene Daten – besonders nun in Ausgestaltung der neuen Portalverbünde – verarbeitet werden, sind spezifische Informationen notwendig. „Eine Datenschutzerklärung für alle Prozesse funktioniert rechtlich nicht. Die Angaben müssen einen eindeutigen Bezug haben, die spezifische Verarbeitung des jeweiligen Prozesses wiedergeben. Informationen und Verweise, die zum Beispiel für „Mein KFZ“ benötigt werden, wären ja in Prozessen der Beurkundung oder der Hundesteuer nur irreführend“, legt Dörte Wilhelms dar. „Deshalb sind wir jeden Standard-Prozess durchgegangen, haben die Anforderungen bereichsübergreifend mit unserem Servicebereich Datenschutz erarbeitet. Entstanden sind prozessuale Datenschutzerklärungsteile, auch für gleichartige Prozesse, die in einer einzigen Datenschutzerklärung beschrieben werden können.“

DATENSCHUTZFOLGE-ABSCHÄTZUNG: DAS FEGEFEUER DES DATENSCHUTZES

Zu den umfangreichen Aufgaben der Datenschutzbeauftragten gehören neben der Prüfung und Gewährleistung von Rechtmäßigkeit, Zweckbindung, Datensparsamkeit und Datensicherheit auch die Beratung bei der Beurteilung von Folgerisiken nach Art. 35 DSGVO. Mittels exakter Beschreibung der geplanten Verarbeitungsvorgänge und der jeweiligen Verarbeitungszwecke personenbezogener Daten erfolgt eine detaillierte und strukturierte Risikoanalyse. „Eigentlich betrachtet man jedes mögliche Szenario, jede einzelne Verarbeitung von Daten. Jeder digitale Prozess ist individuell zu prüfen, aber auch jede Videoüberwachung, jede Bildverarbeitung und auch jeder analoge Vorgang“, führt Klaus Exner aus. Um den Bürger dann vor den angenommenen möglichen Risiken durch die passenden Maßnahmen zu schützen, werden Notwendigkeit und Verhältnismäßigkeit der Datenerhebungen in Bezug auf den Zweck, die Risiken für die Rechte und Freiheiten der betroffenen Personen, sowie die für die Bewältigung der Risiken geplanten Abhilfemaßnahmen und Sicherheitsvorkehrungen systematisch beschrieben und bewertet.

Dabei gilt, je sensibler die Daten, desto höher das mögliche Risiko. „Wir bieten unseren Kunden die komplette Durchführung der Datenschutz-Folgenabschätzung. Dazu gehören die Bewertung des Schutzbedarfs, die Risikobewertung, die Beurteilung der getroffenen Maßnahmen und die Empfehlung weiterer Maßnahmen zum Schutz der personenbezogenen Daten. Und nicht zuletzt die dazugehörige Dokumentation“, ergänzt der Datenschutzexperte.

Die ITEBO-Unternehmensgruppe unterstützt in der Funktion eines externen Datenschutzbeauftragten bei inzwischen über 120 öffentlichen Kunden: Von der Prüfung der rechtlichen Gegebenheiten, der Schwellwertanalyse, den Risikofolgeabschätzungen bis hin zur datenschutzrechtlichen Umsetzung und Sicherung.

