UNABHÄNGIGES DATENSCHUTZ ZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Fritz-Dobisch-Straße 12 . 66111 Saarbrücken
Postfach 10 26 31 . 66026 Saarbrücken
Telefon 0681/94781 – 0
Telefax 0681/94781-29
E-Mail poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de

Unabhängiges Datenschutzzentrum Saarland - Fritz-Dobisch-Str. 12 - 66111 Saarbrücken

Landtag des Saarlandes
Enquêtekommission „Digitalisierung im Saarland“
Franz-Josef-Röder-Straße 7

66119 Saarbrücken

Saarbrücken, 7. Mai 2019

Az:
Bearbeiter/in:
Durchwahl:
E-Mail:

Enquêtekommission „Digitalisierung im Saarland – Bestandsaufnahme, Chancen und Maßnahmen“

Hier: Anhörung zum Thema E-Government

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

zunächst möchte ich mich für die Gelegenheit bedanken, aus datenschutzrechtlicher Sicht im Rahmen der Anhörung der Enquêtekommission zum Thema E-Government Stellung nehmen zu können.

Eine wesentliche Voraussetzung für die Akzeptanz von E-Government-Angeboten der saarländischen Kommunen und denen des Landes durch die Bürger ist ein hohes Datenschutzniveau entsprechender Verfahren. Ein starker Datenschutz stellt damit ein zentrales Element für die erfolgreiche Etablierung von E-Government-Prozessen dar.

E-Government, also die elektronische Abwicklung von Geschäftsprozessen der öffentlichen Verwaltung und Regierung, kommt in Deutschland nur schwerlich in Gang. Nach einer Studie der Initiative D21 für das Jahr 2018[1] ist die Nutzung von E-Government-Angeboten in Deutschland sogar rückläufig. Lediglich 40 Prozent der Befragten gaben an, dass sie in den letzten 12 Monaten E-Government-Angebote genutzt haben, während dies im Jahr 2012 noch 45 Prozent waren.

[1] eGovernment Monitor 2018; Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich (https://www.egovernment-monitor.de).

Dabei ist diese Zurückhaltung der Bundesbürger keineswegs auf die mangelnde Bekanntheit entsprechender Angebote und Dienstleistungen zurückzuführen. Ganz im Gegenteil geben acht von zehn Befragten an, dass sie regelmäßig auf den Internetseiten ihrer Kommune/Stadt nach Informationen bspw. zu Zuständigkeiten und Öffnungszeiten suchen und zeigen somit, dass sie über die Existenz entsprechender Angebote informiert sind.

Betrachtet man hingegen die - neben der Informationssuche - anderen Interaktionsformen im E-Government, so wird deutlich, dass die Nutzung von digitalen Kommunikationswegen mit der Verwaltung ebenso wie die Inanspruchnahme elektronischer Antragsverfahren von den Bürgern nur sehr zurückhaltend angenommen wird. Insbesondere wenn es darum geht die vorhandenen E-Government-Angebote nicht nur im Sinne einer Informationsquelle, sondern durch die Inanspruchnahme digitaler Verwaltungsverfahren zu nutzen, offenbart sich eine starke Diskrepanz zwischen Bekanntheit, Interesse und tatsächlicher Nutzung entsprechender Angebote.

Die Gründe für diese Diskrepanz sind unterschiedlich. Sie haben zum einen ihren Ursprung in organisatorischen Rahmenbedingungen. So stellt bspw. die fehlende Nutzerfreundlichkeit und komplexe Bedienbarkeit entsprechender Angebote eine relevante Nutzungsbarriere dar.

Entscheidender sind jedoch Datenschutzbedenken, die für die Zurückhaltung der Bürger bei der Nutzung von E-Government-Angeboten eine gewichtige Rolle spielen. Für fast jeden Zweiten sprechen Sorgen um Datenschutz und Datensicherheit gegen die Nutzung von E-Government-Angeboten.

Diese Bedenken nehmen in Abhängigkeit der Sensitivität der verarbeiteten Daten zu. So könnte sich noch knapp jeder zweite Befragte vorstellen, in einer staatlichen Online-Plattform (sog. Bürgerkonto) persönliche Unterlagen wie Meldebescheinigungen und Heirats- oder Geburtsurkunden zu speichern. Die digitale Speicherung von privaten Dokumenten, wie Versicherungsunterlagen oder medizinische Unterlagen, in einem solchen Bürgerkonto käme hingegen nur für jeden Fünften in Betracht.

Die Sorgen der Bürger um Datenschutz und Datensicherheit korrespondieren mit entsprechenden Bedrohungsszenarien beim Angebot von E-Government-Angeboten.

So werden beim E-Government oft zentrale, bereichsübergreifende Datenbestände angelegt, um Bürgern und Unternehmen Verwaltungsdienstleistungen unterschiedlicher Behörden oder Behördenbereiche an einer zentralen Stelle oder mit einem elektronischen Verfahren (One-Stop-Government, Lebenslagenkonzept) anbieten zu können. Den daraus resultierenden Bedrohungen, nämlich die Gefährdung der Zweckbindung gespeicherter Datenbestände, die Gefährdung der „informationellen Gewaltenteilung", mangelnde Transparenz für Betroffene (wer greift zu welchem Zweck auf welche Daten zu) und unzulässiges Aufspüren unbekannter

Zusammenhänge mit Data Mining-Technologien muss bereits bei der Planung und Konzeptionierung entsprechender Angebote wirksam begegnet werden („privacy by design", Art. 25 Abs. 1 DSGVO).

Die ständig zunehmende Menge an personenbezogenen Daten und die relativ einfache Zusammenführung von elektronisch gespeicherten Informationen über einzelne Personen kann weiterhin dazu führen, dass Entscheidungen ausschließlich aus der automatischen Bewertung einzelner gespeicherter Persönlichkeitsmerkmale resultieren. Für den Betroffenen kann das bedeuten, dass seine persönlichen Belange und Interessen nicht berücksichtigt werden, weil keine natürliche Person in den Entscheidungsprozess einbezogen wird oder er nicht in der Lage ist, persönliche Interessen geltend zu machen.

E-Government-Anwendungen erfordern elektronische Kommunikation zwischen Bürgern und behördeninternen IT-Systemen. Die hierfür erforderliche „Öffnung" des Verwaltungssystems über entsprechende Schnittstellen kann zu erheblichen Gefährdungen für die Integrität, die Verfügbarkeit und die Vertraulichkeit der bei der Behörde vorhandenen personenbezogenen Daten führen. Schadprogramme wie Viren, Würmer oder Trojanische Pferde können die Rechner und andere Komponenten des Verwaltungsnetzes nachhaltig schädigen. Eine mangelhafte Benutzer- und Rechteverwaltung kann dazu führen, dass Unberechtigten Zugang zu personenbezogenen Daten gewährt wird. Nicht regelmäßig aktualisierte und gewartete Soft- und Hardware, der Einsatz veralteter und damit unsicherer Verschlüsselungs- oder Signaturverfahren oder der nicht ordnungsgemäße Umgang mit Zertifikaten oder geheimen Schlüsseln stellen zusätzlicher Bedrohungsszenarien dar, ermöglichen die Ausnutzung entsprechender Schwachstellen durch externe Angreifer und stellen ein zusätzliches Risiko für die Sicherheit der Verarbeitung personenbezogener Daten dar.

Schließlich dürfen auch die Gefährdungen für Zweckbindung, Verfügbarkeit, Vertraulichkeit und Integrität nicht unberücksichtigt bleiben, die sich aus einem sorglosen Umgang mit personenbezogenen Daten durch die hierzu Berechtigten ergeben. Beispiele hierfür sind unzulässige Übermittlung personenbezogener Daten (fahrlässig oder vorsätzlich) an Dritte, versehentliche Löschung oder Veränderung durch fehlende Sorgfalt bei der Verarbeitung personenbezogener Daten, unzureichende Benutzer- und Rechteverwaltung, fehlende oder unzureichende Zuständigkeitsregelungen für die Pflege zentraler Datenbestände sowie ein zu umfassender Online-Zugriff auf die automatisierten Datenbestände der Behörde (etwa durch einen Behördenleiter).

Um diesen Bedrohungen wirksam zu begegnen, müssen E-Government-Verfahren unter konsequenter Berücksichtigung datenschutzrechtlicher Prinzipien (Art. 8 GRCh, Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG und Art. 5 DSGVO) gestaltet und betrieben werden:

Gewichtung personenbezogener Daten

Personenbezogene Daten sind im Hinblick auf den Schutzbedarf sowohl einzeln als auch im Gesamtkontext der Anwendung zu bewerten. Wirken verschiedene Stellen an der E-Government-Anwendung mit, ist darauf zu achten, dass die Daten der beteiligten Einrichtungen insgesamt bewertet

werden. Die Ausgestaltung der Schutzmaßnahmen muss sich daran orientieren, welche Folgen für einen Betroffenen durch die Beeinträchtigung des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) sowie des Rechts auf Datenschutz (Art. 8 GRCh) entstehen können und welcher potentielle Schaden für den Betreiber eintreten kann.

Erforderlichkeit und Verhältnismäßigkeit

Jede Datenverarbeitung muss sich an dem Grundsatz der Erforderlichkeit orientieren. Die Einhaltung des Erforderlichkeitsgrundsatzes im Einzelfall ist bereits in der Konzeptions- und Planungsphase von E-Government-Anwendungen und bei der Systemauswahl zu berücksichtigen. Insofern korrespondiert die Vorgabe mit den Geboten zur Datenvermeidung und -minimierung (siehe nächster Punkt). Das Gebot der Erforderlichkeit gilt für alle Phasen der Verarbeitung, also nicht nur für die Erhebung, sondern auch für den gesamten anschließenden Verarbeitungsprozess. Daten, die für den weiteren Verwaltungsvollzug ab einer bestimmten Stufe nicht (mehr) erforderlich sind, sind zu löschen oder, wenn sie für bestimmte Kontroll- oder Nachweisfunktionen im Einzelfall noch benötigt werden, zu anonymisieren oder zumindest zu pseudonymisieren. Diese Maßnahmen können von modernen IT-Systemen dynamisch durchgeführt werden, d.h. bei Überschreiten eines bestimmten Termins (Löschfrist, Antragsende, Ablauf der Wirkung eines Verwaltungsaktes) oder bei Eintritt eines bestimmten Ereignisses (der geforderte Nachweis wird erbracht) werden entsprechende Datenfelder gelöscht.

Datenvermeidung und Datenminimierung

Das Gebot der Datenvermeidung und Datensparsamkeit verlangt von der verantwortlichen Stelle eine aktive Gestaltung ihrer technisch-organisatorischen Verfahren in der Form, dass möglichst keine oder so wenig personenbezogene Daten wie möglich verarbeitet werden. Über das Erforderlichkeitsprinzip hinaus fordert es von der verantwortlichen Stelle, die Umstände der Erforderlichkeit, die Zwecke und Prozesse der Datenverarbeitung zu überprüfen und mit dem Ziel der Vermeidung von Daten oder ihres Personenbezugs zu gestalten.

Rechtsgrundlage für die Datenverarbeitung, elektronische Einwilligung

Jede Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen bedarf einer gesetzlichen Rechtfertigung aus der sich Art, Umfang und Zweck der Verarbeitung ergeben. Bei fehlender einschlägiger Rechtsvorschrift kann diese fehlende gesetzliche Befugnis grundsätzlich nicht durch eine Einwilligung des Betroffenen ersetzt werden, da es insbesondere im Bereich der Hoheitsverwaltung auf Grund des zwischen dem Bürger und der Behörde existierenden strukturellen Ungleichgewichts an der für die Wirksamkeit der Einwilligung notwendigen Freiwilligkeit der Willensentschließung fehlen wird (Art. 7 Abs. 4 DSGVO). Kann die Verarbeitung ausnahmsweise doch auf eine Einwilligung des Betroffenen gestützt werden, so darf die Datenverarbeitung nur mit vorheriger, ausdrücklicher Zustimmung des Betroffenen erfolgen. Die Einwilligung bei E-Government-Anwendungen kann dabei auch elektronisch erklärt werden.

Sicherung der Zweckbindung

Da bei E-Government-Anwendungen verknüpfbare Sammlungen von personenbezogenen Daten entstehen, muss besonders darauf geachtet werden, dass diese Daten wirklich nur für die konkreten Zwecke verwendet werden, für die sie erhoben und gespeichert wurden. Nur in für den Bürger klar überschaubaren Grenzen, nämlich aufgrund einer ausdrücklichen gesetzlichen Erlaubnis oder mit Einwilligung des Betroffenen, dürfen diese Daten auch für andere Zwecke verwendet werden. Die Zweckbindung muss vorsorglich durch organisatorische und technische Maßnahmen gesichert werden.

Transparenz

Nur wenn die Bürgerinnen und Bürger wissen, wie die Datenverarbeitungsvorgänge ablaufen, haben sie auch die Möglichkeit, ihre Rechte wahrzunehmen. Für viele Nutzer wird allerdings nicht ohne weiteres erkennbar sein, an welchen Stellen sie bei Nutzung elektronisch zur Verfügung gestellter Informationen Spuren hinterlassen bzw. inwieweit personenbezogene Nutzerdaten weiterverarbeitet werden. Daher müssen die Nutzer zu Beginn des Verfahrens, sowie bei jeder Zweckänderung über Art, Umfang und Zwecke der Verarbeitung unterrichtet werden. Nur die Vorabinformation versetzt die Nutzer in die Lage darüber zu entscheiden, ob und in welchem Umfang sie dazu bereit sind, E-Government-Anwendung unter Angabe personenbezogener Daten zu nutzen.

Systemdatenschutz

Durch eine gezielte Gestaltung der Systeme und Verfahren zur Verarbeitung personenbezogener Daten soll erreicht werden, dass die Ziele des Datenschutzrechts durch die Technik selbst gewährleistet werden. Durch Systemdatenschutz sollen Datenschutzrisiken durch Maßnahmen zur Datenvermeidung und Datensparsamkeit reduziert, informationelle Gewaltenteilung durch Verteilung von Verarbeitungsprozessen, und Datenbeständen verwirklicht, die Integrität, Authentizität, Vertraulichkeit und Verfügbarkeit der Daten durch Maßnahmen der Datensicherheit gewährleistet und die infrastrukturellen Voraussetzungen für die Wahrnehmung von Betroffenenrechten geschaffen werden.

Grundlegend für die Akzeptanz von E-Government-Anwendungen ist Vertrauen in die entsprechenden Verfahren. Dieses muss durch ausgeprägten Datenschutz, datensparsames Systemdesign, Aufklärung der Nutzer und durch wirksame IT-Sicherheitsmaßnahmen gestärkt werden. Nicht die Reduzierung des Datenschutzniveaus oder gar die Absenkung datenschutzrechtlicher Anforderungen durch legislative Maßnahme zur Ermöglichung einer kostengünstigen und schnellen Einführung von neuen elektronischen Verwaltungsverfahren sind die Faktoren für ein erfolgreiches E-Government, sondern im Gegenteil eine frühzeitige, dauerhafte und konsequente Berücksichtigung datenschutzrechtlicher Rahmenbedingungen. Hierzu sollte der bestehende, durch die Datenschutz-Grundverordnung vorgegebene Rechtsrahmen genutzt werden. Politische Forderungen nach einer größeren Nutzbarmachung von immer mehr Daten, die den Datenschutz als ein Konzept aus dem 18. Jahrhundert darstellen, kombiniert mit Appellen, dem Staat doch die gleichen Verarbeitungsmöglichkeiten wie der Wirtschaft

zur Verfügung zu stellen wirken hier eher kontraproduktiv und fördern das ohnehin bestehende Misstrauen der Bürger.

Bei der Einführung von E-Government-Anwendungen ist auch die Einbeziehung der Datenschutzaufsichtsbehörden nicht zu vergessen, da diesen die Überwachung und Kontrolle der Einhaltung datenschutzrechtlicher Bestimmungen obliegt. Eine umfassende Einbindung der Datenschutzaufsichtsbehörde in die Planung, Konzeptionierung und Einführung von neuen E-Government-Verfahren, wie dies in Art. 57 Abs. 1 lit. c DSGVO und § 19 Abs. 2 Satz 1 SDSG vorgesehen ist, sowie die regelmäßige Einbeziehung bei der Evaluierung bereits existierender Verfahren gewährleistet eine unabhängige Bewertung des Datenschutzniveaus neuer und bestehender E-Government-Anwendungen. Die Datenschutzaufsichtsbehörde kann damit als neutrale Instanz einen erheblichen vertrauensstiftenden Beitrag leisten. Dies setzt jedoch eine angemessene Ausstattung mit personellen, sachlichen und finanziellen Mitteln voraus.

Zusammenfassend bleibt festzuhalten, dass ein starker Datenschutz wesentliches Element für die erfolgreiche Etablierung von E-Government-Angeboten sein muss.

Gerne stehe ich Ihnen für weitere Erläuterungen oder Rückfragen zur Verfügung.

Mit freundlichen Grüßen

Monika Grethel
Landesbeauftragte für Datenschutz
und Informationsfreiheit