Appenzell Ausserrhoden

Datenschutz-Kontrollorgan

Poststrasse 23
9001 St. Gallen

Stefan Gerschwiler
lic. iur., Rechtsanwalt
Tel. 071 228 29 30
stefan.gerschwiler@ar.ch

Datenschutz-Kontrollorgan, 9001 St. Gallen

An den Kantonsrat

St. Gallen, 29. Februar 2024

Bericht 2023 des Datenschutz-Kontrollorgans

Sehr geehrter Herr Kantonsratspräsident
Sehr geehrte Damen Kantonsrätinnen
Sehr geehrte Herren Kantonsräte

Gerne berichte ich (im Sinne von Art. 27 Abs. 1 Bst. h DSG) über meine Tätigkeit als Datenschutz-Kontrollorgan im Jahr 2023.

A. Tätigkeitschwerpunkte

1. Beratung von öffentlichen Organen

Im Berichtsjahr zeigte sich eine leichte Zunahme von Beratungsanfragen öffentlicher Organe (Berichtsjahr: 65, Vorjahr: 60).

Ein die Beratungstätigkeit prägender Faktor waren über das ganze Jahr Cybersicherheitsvorfälle bei externen Informatikdienstleistern, in der Schweiz und weltweit. Sie bildeten ein Umfeld ab, das der Nachrichtendienst des Bundes (NDB) in seinem aktuellen Lagebericht "Sicherheit Schweiz 2023" folgendermassen beschreibt: "Die Bedrohung der Schweiz durch ausländische, hauptsächlich russische und chinesische Spionage bleibt hoch" "und "Dass meist finanzielle Motive hinter den festgestellten Cyberangriffen stehen, schliesst andere Motive nicht aus. Gewalttätig-extremistische, terroristische, nachrichtendienstliche oder machtpolitische Motive sind auch möglich".

Appenzell Ausserrhoden

Im Juni 2023 teilte der Bundesrat mit, bei der Schweizer Firma Xplain seien "grosse Datenmengen" gestohlen worden. Das Unternehmen ist auf die Entwicklung von Softwarelösungen für Behörden spezialisiert. Zu seinen Kunden gehören etwa die Bundesämter für Polizei und für Zoll und Grenzsicherheit. Entwendet wurden z.B. Daten zu zivilen und militärischen Strafverfahren, aus dem Informationssystem "HOOGAN" sowie Log-Dateien und Fehlerberichte eines Systems des Bundes, das zur Erfassung von biometrischen Daten wie Fingerabdrücken und Gesichtsbildern benutzt wird. Hinter dem Angriff steckte die Bande Play, die sich auf den Diebstahl von Daten und Erpressung ("Ransomware") spezialisiert hat. Neben Xplain sind im Jahr 2023 mehrere Institutionen in der Schweiz, darunter die Gemeinde Saxon VS und die Medienhäuser NZZ und CH Media, Ziel ihrer Angriffe geworden.

Im Juli 2023 meldete die Firma Microsoft, sie habe Angriffe chinesischer Akteure auf Kunden-E-Mails in ihrer Azure Cloud entdeckt. Gestohlen wurden insbesondere rund 60'000 E-Mails aus verschiedenen Konten des U.S. State Departement[1].

Im November 2023 informierte das Eidgenössische Finanzdepartement über einen Ransomware-Angriff auf die Firma Concevis, eine Schweizer Anbieterin von Softwarelösungen für öffentliche Verwaltungen (Bund, Kantone, Städte), den Finanzsektor und Unternehmen aus der Industrie und Logistik. Zu den Kunden von Concevis gehören unter anderen das Bundesamt für Bevölkerungsschutz, das Bundesamt für Statistik, das Bundesamt für Zivilluftfahrt, die Eidgenössische Steuerverwaltung und das Kommando Ausbildung. Die Angreifer entwendeten Daten und verschlüsselten danach sämtliche Server der Firma. Nachdem diese der Lösegeldforderung nicht nachgekommen ist, drohen die Angreifer mit der Veröffentlichung der Daten im Darknet.

Auch Microsoft war nach eigenen Angaben[2] im November 2023 erneut betroffen: Eine vom russischen Staat unterstützte Hackergruppe habe sich Zugriff auf E-Mail-Konten verschafft, darunter solche von Führungskräften und Mitarbeitern der Bereiche Cybersicherheit und Recht. Es seien E-Mails und angehängte Dokumente entwendet worden.

Neben den geschilderten Angriffen gelangen Akteure auch ganz formal auf dem Rechtsweg an fremde Daten bei IT-Anbietern. So forderten z.B. US-amerikanische Regierungsstellen von Microsoft im Jahr 2022 gestützt auf "Foreign Intelligence Surveillance Act Orders" Inhaltsdaten von zwischen 20'500 und 21'999 Konten an[3]. Ob bzw. wie viele Schweizer Konten betroffen waren, darf Microsoft nicht kommunizieren; offen bleibt auch, was unter einem "Konto" bzw. "account" genau zu verstehen ist (einzelne natürliche Person, ganze Geschäfts-/Behördenkunden?).

Appenzell Ausserrhoden war von diesen Vorfällen nach meinen Abklärungen nicht direkt betroffen. Das war zum Teil allerdings auch schlicht Glück. Die geschilderten Beispiele zeigen jedenfalls, dass die Auslagerung von Datenbearbeitungen an Dritte im In- und Ausland heute technische Realität ist, auch und insbesondere bei der öffentlichen Verwaltung; das gilt auch für unseren Kanton. Auslagerung geht immer mit gewissen Risiken für Kontrollverlust über die bearbeiteten Daten einher, die nicht einfach abstrakt bestehen, sondern sich auch regelmässig konkret realisieren. Rechtlich gilt dabei: Auslagern lässt sich zwar der technische Betrieb, nicht

[1] https://www.reuters.com/world/us/chinese-hackers-stole-60000-emails-us-state-department-microsoft-hack-senate-2023-09-27/
[2] https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/
[3] https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report; vgl. auch die Angaben zu weiteren Anfragen durch Strafverfolgungsbehörden hier: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

Appenzell Ausserrhoden

aber die Verantwortung für den Datenschutz. Ihre Verantwortung haben öffentliche Organe namentlich dadurch wahrzunehmen, dass sie ihre IT-Partner sorgfältig auswählen, instruieren und überwachen.

Diese unübertragbare Verantwortung ist manchmal nur schwierig in Einklang zu bringen mit dem an sich berechtigten und nachvollziehbaren Anspruch öffentlicher Organe (und der Bürgerinnen und Bürger), dass IT-Dienste sicher, einfach, jederzeit und überall verfügbar sein sollen. Das zeigte sich etwa auch in der Bandbreite der Rückmeldungen zur Cloud-Ergänzung der eGovernment- und Informatik-Strategie 2021 (vgl. meinen Bericht 2022, S. 1), deren Genehmigungsverfahren noch nicht abgeschlossen ist.

Die rege Nutzung meines Beratungsangebots zeugt davon, dass die öffentlichen Organe in Appenzell Ausserhoden ganz überwiegend interessiert und willens sind, ihre datenschutzrechtliche Verantwortung wahrzunehmen. Als ein positives Beispiel aus dem Berichtsjahr möchte ich das Departement Gesundheit und Soziales DGS hervorheben, wo ich im Rahmen einer Kadertagung Gelegenheit zum direkten Austausch über aktuelle Themen und Herausforderungen im Bereich des Datenschutzes hatte. Die Vielzahl und Breite der dort (und im Berichtsjahr in anderen Zusammenhängen) erörterten Fragestellungen einerseits und der für die betroffenen Personen regelmässig sehr bedeutsame Inhalt der der im Verantwortungsbereich des DGS bearbeiteten Daten (Angaben zur Gesundheit) anderseits, lassen aus meiner Sicht folgenden Schluss zu: Der Auf- und Ausbau von eigener Fachkompetenz im Bereich Datenschutz, beispielsweise auf Stufe Departementssekretariat / Rechtsdienst, könnte beim DGS (wie z.B. auch beim Departement Inneres und Sicherheit, das sich vergleichbaren Herausforderungen gegenüber sieht) mittelfristig dazu beitragen, dem anspruchsvollen technischen und rechtlichen Umfeld auch weiterhin angemessen zu begegnen.

Folgende Beispiele mögen einen Eindruck über die Bandbreite der an mich im Berichtsjahr herangetragenen und beurteilten Fragen geben, wobei in allen Fällen nach meiner Einschätzung datenschutzrechtlich korrekte Lösungen gefunden werden konnten bzw. können: Die Kantonskanzlei führte für den Regierungsrat unter Beizug eines externen Dienstleisters eine Bevölkerungsbefragung durch und benötigte dazu Daten aus den Einwohnerregistern der Gemeinden. Das Personalamt führt kantonsweit ein elektronisches Personaldossier ein. Die Sozialversicherungen Appenzell Ausserrhoden wechselten den Software-Anbieter ihrer zentralen Fachapplikation. Der Kanton baut ein Webportal für digitale Behördendienstleistungen auf. Das Strassenverkehrsamt beteiligt sich an einem Pilotversuch für einen digitalen (Lern-)Führerausweis. Die Kantonspolizei hat ihre Posten in Heiden und Teufen mit Videoüberwachungsanlagen ausgestattet.

Nicht zuletzt konnten wir am runden Tisch bzw. in Arbeitsgruppen unter Einbezug verschiedener betroffener Stellen Lösungen für die Übermittlung von Informationen aus dem Bereich des Steuerbezugs (Debitorenlisten) durch die Kantonale Steuerverwaltung an die Gemeinden und für den Datenfluss zwischen KESB und Einwohnerkontrollen erarbeiten.

2. Zusammenarbeit mit anderen Kantonen und Bund

Die Konferenz der schweizerischen Datenschutzbeauftragten (privatim) hat an ihrem Herbstplenum 2023 den Beschluss gefasst, eine Informationsplattform für den gegenseitigen Austausch zu entwickeln und bei der Digitalen Verwaltung Schweiz (DVS) einen Antrag auf Mitfinanzierung zu stellen. Davon wird auch Appenzell Ausserrhoden profitieren.

Appenzell Ausserrhoden

Die bestehende, gut funktionierende informelle Zusammenarbeit im Rahmen des Erfahrungsaustausches der Ostschweizer Datenschutzbehörden bildete Gegenstand eines Beratungsprozesses durch einen externen Gutachter. Dieser wurde durch die Kantone Appenzell Ausserrhoden, Appenzell Innerrhoden, St. Gallen und Thurgau eingesetzt. Er hat, unter Einbezug der Datenschutzbehörden, Vorschläge für eine weitere Optimierung und Vertiefung der Zusammenarbeit unterbreitet und wird diese weiter konkretisieren.

3. Beratung von Privaten

Die Beratungsanfragen von Privaten haben im Berichtszeitraum um rund einen Drittel zugenommen.

Ein Grund dürfte das Inkrafttreten des revidierten Datenschutzgesetzes des Bundes per 01.09.2023 gewesen sein. Das Thema Datenschutz wurde dadurch in der öffentlichen Diskussion und Wahrnehmung aktuell und führte zu einer erhöhten Sensibilisierung.

Rechtlich sind die Auswirkungen dieser Revision auf Bundesebene für die öffentliche Verwaltung in Appenzell Ausserrhoden klein, insbesondere im Vergleich zur laufenden Totalrevision unseres kantonalen Datenschutzgesetzes. Viele Eckpunkte unserer kantonalen Revisionsvorlage sind, wegen staatsvertraglicher Vorgaben, aber ähnlich wie die beim Bund nun vorgenommen Anpassungen.

Obwohl bei uns nicht direkt anwendbar, sind doch die im Zuge der Gesetzesrevision ebenfalls erfolgten Konkretisierungen in gewissen Bereichen des Datenschutzrechts durch den Bundesrat auf Verordnungsstufe und durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten für die Praxis relevant. Ich lehne mich bei meiner Tätigkeit regelmässig daran an.

B. Aufsichts- und Kontrolltätigkeit

In meiner Aufsichtstätigkeit beobachte ich in einzelnen Fällen, dass der angemessene Umgang mit Risiken beim Beizug von IT-Dienstleistern (siehe oben, Abschnitt A.) nicht hinreichend Beachtung erfährt. So kommt es vor, dass aus der blossen Beliebtheit und Verbreitung von Software der Schluss gezogen wird, diese könne bedenkenlos durch öffentliche Organe eingesetzt werden. Dieser Schluss ist gefährlich, jedenfalls ist er falsch.

Als konkretes Beispiel diene folgender Fall: Die Produkte des Anbieters Meta (z.B. Facebook, Whatsapp, Instagram) sind beliebt und verbreitet. Das sehr erfolgreiche Geschäftsmodell basiert auf dem Prinzip, dass die Nutzer nicht direkt mit Geld bezahlen, sondern dass Meta alle bei der Nutzung seiner Produkte anfallenden Daten (also z.B.: Wer kommuniziert mit wem, worüber, wie häufig, etc.) ganz umfassend auswertet und dies bei Dritten (Werbekunden) zu Geld macht. Als Folge dieses Geschäftsmodells sieht sich der Konzern seit Jahren im Herkunftsland USA und weltweit mit Gerichtsverfahren im Bereich des Datenschutzrechts bzw. der Daten-

Appenzell Ausserrhoden

schutz- und Wettbewerbsaufsicht konfrontiert. Anfangs 2023 verhängte etwa die irische Datenschutzaufsichtsbehörde Bussen von € 210 Mio. (Facebook), € 180 Mio. (Instagram) und € 5.5 Mio. (WhatsApp). Im Mai 2023 kam, auf Beschluss des Europäischen Datenschutzausschuss (EDSA), eine weitere Busse von € 1.2 Mrd. (nicht Mio.!) dazu. Im selben Monat teile die US-Handelsaufsicht FTC (Federal Trade Commission) mit, sie sehe wegen neuer Verstösse vor, das 2019 mit einer Rekordstrafe von fünf Milliarden US-Dollar und umfangreichen Auflagen abgeschlossene Verfahren wiederzueröffnen. Die FTC will für 20 Jahre strengere Auflagen verhängen sowie komplett untersagen, dass Meta Daten Minderjähriger für kommerzielle Zwecke nutzt.

Die Beratungsstelle für Suchtfragen Appenzell Ausserrhoden hat im Berichtsjahr Meta als (einen) IT-Anbieter für ihre Dienstleistungen ausgewählt. Sie hat dabei keinerlei Abklärungen zum Datenschutz vorgenommen, keine Alternativen evaluiert und auch keine Vereinbarungen mit Meta getroffen. Die Wahrscheinlichkeit, dass Meta im Zusammenhang mit der Suchtberatung anfallende Daten für eigene wirtschaftliche Zwecke aus- und verwertet, kann die Beratungsstelle nach eigener Aussage nicht einschätzen. Sie sehe aber "keine Risiken betreffend Verletzung der Grund- und Persönlichkeitsrechte". Diese Einschätzung teile ich nicht, zumal jedenfalls keineswegs ausgeschlossen ist, dass Personen, die auf dem von Meta zur Verfügung gestellten Kommunikationskanal Suchtberatung in Anspruch nehmen, gezielt Werbung von z.B. Online-Casinos oder Wettbüros angezeigt wird.

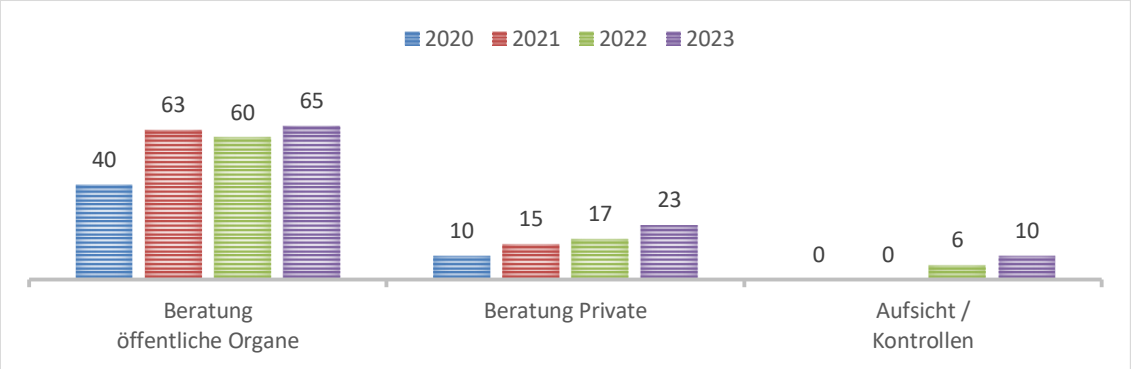
Wenn öffentliche Organe ihre Verantwortung zur sorgfältigen Auswahl, Instruktion und Überwachung ihrer IT-Dienstleister nicht wahrnehmen, riskieren sie nach meiner Einschätzung, Vertrauen der Bürgerinnen und Bürger zu verlieren. Nach meiner Wahrnehmung legen breite Teile der der Bevölkerung durchaus Wert darauf, dass mit ihren Daten angemessen umgegangen wird. Dass die Nachfrage nach Suchtberatung über den Kommunikationskanal von Meta "geringer" ausfällt, "als angedacht", mag Ausdruck davon sein. Jedenfalls soll das Angebot "im Jahr 2024 einer Evaluation" unterzogen werden.

Die Auswertung der Zugriffe auf die kantonale Einwohnerdatenplattform (vgl. meinen Bericht 2022, S. 3) hat ergeben, dass aus zwei Betreibungsämtern auffallend hohe Zugriffszahlen zu verzeichnen waren. Diese Zugriffe konnten durch die mir dargestellten Arbeitsabläufe indes plausibilisiert werden. Weiterer Handlungsbedarf besteht aus meiner Sicht im Moment nicht.

Appenzell Ausserrhoden

C. Ressourcen / Entwicklung

Die Entwicklung der Fallzahlen in den einzelnen Aufgabenbereichen lässt sich grafisch folgendermassen abbilden:



D. Schlussbemerkungen und Antrag

Ich ersuche Sie, sehr geehrter Herr Kantonsratspräsident, sehr geehrte Damen Kantonsrätinnen und Herren Kantonsräte, vom vorliegenden Bericht wohlwollend Kenntnis zu nehmen,

und entbiete an dieser Stelle Ihrer GPK, Ihrer KIS, dem Parlamentsdienst, der Kantonskanzlei, dem Departement Inneres und Sicherheit, dem Departement Finanzen, dem Departement Gesundheit und Soziales, der Informatikstrategie-Kommission und der AR Informatik AG meinen besonderen Dank für die gute Zusammenarbeit bei der Gewährleistung des Datenschutzes in Appenzell Ausserrhoden im Berichtsjahr.

Datenschutz-Kontrollorgan

St. G

Stefan Gerschwiler