KANTON AARGAU

BEAUFTRAGTE FÜR ÖFFENTLICHKEIT UND DATENSCHUTZ

22. Dezember 2023 /ÖDB 23.170

EMPFEHLUNG

Departement Volkswirtschaft und Inneres

öffentliches Organ,

betreffend: Meldung Datensicherheitsverletzung Xplain AG

1.

Ende Mai 2023 wurde bekannt, dass die Schweizer Xplain AG, eine Anbieterin von Behördensoftware, Opfer eines Ransomware-Angriffs durch die Hackergruppe "Play" geworden war. Betroffen vom Ransomware-Angriff auf die Firma Xplain AG waren auch Daten, die im Rahmen von Softwareentwicklungsprojekten zwischen dem Departement Volkswirtschaft und Inneres (DVI) und Xplain AG auf der Infrastruktur von Xplain AG gespeichert waren. Da Xplain AG in Absprache mit den Strafverfolgungsbehörden und dem National Cyber Security Center (NCSC), kein Lösegeld an die Hacker bezahlte, veröffentlichten diese die Daten in zwei Schritten am 1. Juni und am 14. Juni 2023 im Darknet.

2.

Die Beauftragte für Öffentlichkeit und Datenschutz (Beauftragte, ÖDB) wurde vom DVI am 24. Mai 2023 mündlich und am 12. Juni 2023 schriftlich über die Datenschutzverletzung bei Xplain AG informiert. Sie erhielt eine Abschlussmeldung des DVI vom 15. Dezember 2023 betreffend Datensicherheitsverletzung Xplain AG (samt Berichten), den Bericht des DVI an den Regierungsrat vom 16. September 2023, die Beantwortung des Regierungsrats der Interpellation Bodmer vom 22. November 2023 samt Medienmitteilung vom 1. Dezember 2023 sowie die Einschätzungen des NCSC vom 16. November 2023 zum Xplain Audit.

Die Meldung der Datensicherheitsverletzung ist damit abgeschlossen. Zu folgendem Punkten sind ergänzende und präzisierende Empfehlungen abzugeben:

2.1

Veröffentlicht wurden geschäftliche Kontaktdaten von Mitarbeitenden des Amts für Migration und Integration des Kantons Aargau (MIKA) und der Kantonspolizei, Kontaktdaten von Gemeinden, Sozialdiensten und anderen Organisationen, Datenextrakte aus den Vorgängersystemen des MIKA, betriebliche Scans und Screenshots von Kundenbeziehungen, einzelne gescannte Verfügungen,

Strafbefehle, Gerichtsentscheide und Verwaltungsentscheide, Benutzerhandbücher, Architekturbeschreibungen, Software-Spezifikationen, ISDS-Konzepte, Mustervorlagen mit Personendaten, Fehlerreports und Zugangsdaten zu einzelnen Umsystemen (beispielsweise Zentrales Migrationsinformationssystem [ZEMIS], Kantonales Einwohnerregister [GERES]) sowie von JustThis (Geschäftsverwaltung Strafjustiz) und Polaris (Geschäftsverwaltung Polizei) sowie zur Wartung der Systeme. Dabei handelt es sich auch um produktive, besonders schützenswerte Personendaten. Diese Daten waren von Abteilungen des DVI beziehungsweise der Kantonspolizei an Xplain AG übermittelt worden.

a)

Lässt ein öffentliches Organ Personendaten durch Dritte bearbeiten, hat es den Datenschutz durch Vereinbarungen, Auflagen oder in anderer Weise sicherzustellen (§ 18 Abs. 1 IDAG[1]). Die Bearbeitung von besonders schützenswerten Personendaten ausserhalb der kantonalen IT-Infrastruktur war in den Verträgen mit Xplain AG nicht vorgesehen und dementsprechend wurden Xplain AG auch keine Vorgaben zur Gewährleistung der Datensicherheit bei der Bearbeitung besonders schützenswerter Personendaten gemacht. Art. 8.1.2 der Allgemeinen Geschäftsbedingungen des Kantons Aargau über die Informationssicherheit und den Datenschutz (ISDS) bei der Erbringung von Informatikdienstleistungen (AGB ISDS) sieht im Gegenteil explizit vor, dass Produktivdaten unter keinen Umständen zu Testzwecken benutzt werden dürfen. Das DVI macht zwar geltend, produktive Daten seien nie zu Testzwecken, sondern zur Softwareentwicklung, unter anderem zur Datenmigration aus Vorgängersystemen, an den Dienstleister übermittelt worden. Dies ändert an der Schutzbedürftigkeit der Daten jedoch nichts. Die Übermittlung von Produktivdaten, insbesondere von besonders schützenswerten Personendaten an Xplain AG war daher unzulässig.

b)

Der Grundsatz der Verhältnismässigkeit verlangt, dass eine Massnahme für das Erreichen des im öffentlichen oder privaten Interesse liegenden Zieles geeignet und erforderlich ist und sich für die Betroffenen in Anbetracht der Schwere der Grundrechtseinschränkung als zumutbar erweist. Es muss eine vernünftige Zweck-Mittel-Relation vorliegen (BGE 143 I 403 E. 5.6.3 S. 412 mit Hinweisen; 138 I 331 E. 7.4.3.1 S. 346).

Erforderlich ist eine Massnahme, wenn der angestrebte Erfolg nicht durch gleich geeignete, aber mildere Massnahmen erreicht werden kann (BGE 143 I 403 E. 5.6.3 S. 412; 140 I 218 E. 6.7.1 S. 235). Im Bereich des Datenschutzes heisst dies unter anderem, dass Daten nur dann und nur soweit bearbeitet werden dürfen, als es für den Zweck der Datenbearbeitung notwendig ist (Prinzip der Datenvermeidung und Datensparsamkeit; Urteil des Bundesgerichts 2C_369/2021 vom 22. September 2021 E. 6; BGE 138 I 331 E. 7.4.2.3 S. 345 f.; Urteil des Bundesgerichts 2C_171/2016 vom 25 August 2016 E. 4.1; PHILIPPE MEIER, Protection des données. Fondements, principes généraux et droit privé, Bern 2011, N. 633 und 661 ff.; PASSADELIS/ROSENTHAL/THÜR, Datenschutzrecht, 2015, N. 3.79; MAURER-LAMBROU/STEINER, Basler Kommentar des Datenschutzgesetzes und Öffentlichkeitsgesetzes, 3. Aufl. 2014, N. 11 ad Art. 4 DSG; vgl. auch Art. 4 Abs. 2 DSG und die Konkretisierung dieses Grundsatzes in § 9 IDAG/AG).

Vor der Auslagerung einer Datenbearbeitung hat das verantwortliche Organ daher zu prüfen, ob die Erbringung der Dienstleistung einen Zugriff des Auftragnehmers auf Personendaten erfordert oder ob der Zweck des Auftrags auch erfüllt werden kann, ohne dass der Dienstleister von den Personendaten Kenntnis nimmt, sei es durch Verschlüsselung der Personendaten, Verwendung von anonymisierten, pseudonymisierten oder Testdaten, etc.. Ist die Kenntnis des Auftragnehmers von produktiven Personendaten zur Erfüllung von dessen Auftrag nicht notwendig, ist die Übermittlung dieser Daten an ihn unzulässig, auch wenn der Auftragnehmer zur Geheimhaltung verpflichtet wurde und

[1] Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 (SAR 170.500).

selbst wenn die Daten sehr gut geschützt wären. Es ist daher zwar notwendig, aber noch nicht ausreichend, wenn bestehende Verträge mit Dienstleistern daraufhin überprüft werden, ob genügende Vorgaben zur Informationssicherheit und Datenschutz gemacht werden.

c)

Das Departement Volkswirtschaft und Inneres DVI gibt folgende Gründe für die Übermittlung von Personendaten an Xplain AG an:

- Zur Veranschaulichung der durch JustThis abzulösenden Systeme/Fachanwendungen (mit Funktionalität und den unterstützten Arbeitsprozessen) und zum Verständnis der von Kunden gestellten Anforderungen.
- Zur Spezifikation der Umsetzung neuer Anforderungen und für Optimierungen des bereits umgesetzten Systems.
- Für die Entwicklung von technischen Schnittstellen zu Drittsystemen.
- Für die automatisierte Übernahme von Daten aus den abzulösenden Systemen.
- Stammdaten zur Parametrisierung und Konfiguration des neuen Systems.
- Zur Aufzeichnung, Analyse und Behebung von Fehlern

Das DVI hat nicht eingehender abgeklärt, ob die aufgeführten Gründe tatsächlich eine Übermittlung von Produktivdaten an Xplain AG erforderten oder ob die Ziele auch auf der Infrastruktur des Kantons oder durch Verwendung von Test- oder anonymisierten Daten hätten erreicht werden können. Es beschränkt sich auf die pauschale Feststellung, dass "mehr Daten auf der Infrastruktur der Verwaltung hätten belassen werden können" (Bericht vom 16. September 2023, Ziff. 3.1). Selbst wenn die genannten Gründe zum Teil eine Übermittlung von Produktivdaten an Xplain AG erforderten haben sollten, wurden nach Auftauchen des Bedürfnisses zu Datenübermittlung nicht die notwendigen Schritte zur Gewährleistung der Datensicherheit getroffen. Vor der Übermittlung hätte geprüft werden müssen

- ob einer Auslagerung rechtliche Gründe entgegenstanden;
- ob die Ziele nur durch Übermittlung von Produktivdaten an Xplain AG erreicht werden konnten und nicht auf persönlichkeitsschonendere Art;
- welches der Schutzbedarf der (neu) zu übermittelnden Daten war;
- welches die Risiken der Übermittlung und Speicherung der Produktivdaten bei Xplain AG waren;
- ob die technischen und organisatorischen Massnahmen der Xplain AG zur Gewährleistung der Datensicherheit einen dem Schutzbedarf und den Risiken angemessenen Schutz boten.

Gestützt auf diese Abklärungen hätten die notwendigen vertraglichen Vereinbarungen mit Xplain AG getroffen und entsprechend der Sensibilität der Daten angepasste Vorgaben zur Gewährleistung der Datensicherheit gegeben werden müssen. Deren Einhaltung hätte periodisch kontrolliert werden müssen.

d)

Die gesetzliche Pflicht der öffentlichen Organe, die Datensicherheit auch bei Auslagerung von Datenbearbeitungen durch Auflagen oder vertragliche Vereinbarungen zu gewährleisten, besteht seit Inkrafttreten des IDAG am 1. Juli 2008. Seit 1. August 2018 sieht § 6 VIDAG[2] vor, dass nicht nur vor Einführung einer informatikgestützten Anwendung, sondern auch bei jeder Erweiterung die voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt, eine Datenschutz-Folgenabschätzung durchzuführen ist. Ein solches Risiko ist insbesondere anzunehmen, wenn besonders schützenswerte Personendaten bearbeitet werden, Bearbeitungen von Personendaten durch Auftragnehmende durchgeführt werden oder zwei oder mehrere Organe Personendaten in einem gemeinsamen elektronischen System bearbeiteten. Als Erweiterung sind Änderungen zu betrachten, die zu einer geänderten Rechts- oder Risikolage führen.

Die Beauftragte empfiehlt gestützt auf § 32 Abs. 3 IDAG, die internen Prozesse des DVI daraufhin zu überprüfen, ob die rechtzeitige Durchführung von Datenschutz-Folgenabschätzungen darin genügend verankert ist.

2.2

Dem Aspekt der Kontrolle wird im Abschlussbericht zu wenig Beachtung geschenkt. Es gibt folgende Problembereiche:

- Im Rahmen der internen Dienstaufsicht wurde nicht bemerkt, dass unzulässige Datenbekanntgaben durch die verantwortlichen Stellen an Xplain AG erfolgten.
- Die verantwortlichen Stellen haben die Einhaltung der vertraglichen Vereinbarungen mit Xplain AG nicht direkt (oder durch Ersatzmassnahmen wie externe Audits) überprüft und diese fehlende Kontrolle wurde wiederum von der internen Dienstaufsicht nicht bemerkt.
- Die Verantwortlichkeiten für die interne Kontrolle der Einhaltung der Datenschutzvorschriften sind nicht genügend bekannt. Dies geht aus der Antwort des Regierungsrats vom 22. November 2023 (zu Frage 9) auf die Interpellation Bodmer et. Al. hervor, die keine operativen Verantwortlichen für die Gewährleistung der Datensicherheit benennen kann, sondern die Beauftragte für Öffentlichkeit und Datenschutz sowie die Finanzkontrolle anführt, welche beide keine operative Verantwortung tragen.

Die Beauftragte empfiehlt gestützt auf § 32 Abs. 3 IDAG, die Verantwortlichkeiten betreffend Kontrolle der Einhaltung der Datenschutzvorschriften zu klären.

3.

Stellt die beauftragte Person für Öffentlichkeit und Datenschutz fest, dass Vorschriften über das Öffentlichkeitsprinzip oder über den Datenschutz verletzt werden, kann sie den verantwortlichen öffentlichen Organen eine Empfehlung abgeben. Das öffentliche Organ hat zu erklären, ob es der Empfehlung folgen wird. Lehnt das öffentliche Organ die Befolgung der Empfehlung ab oder entspricht es dieser nicht, kann die beauftragte Person für Öffentlichkeit und Datenschutz die Empfehlung ganz oder teilweise als Verfügung erlassen (§ 32 Abs. 3 und 4 IDAG)

Die Beauftragte sorgt für eine geeignete Publikation der Empfehlungen, vorzugsweise im Internet (§ 20 VIDAG).

---

[2] Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26. September 2007 (SAR 150.711).

Aus diesen Gründen wird

empfohlen:

1. Die internen Prozesse des DVI sind daraufhin zu überprüfen, ob die rechtzeitige Durchführung von Datenschutz-Folgenabschätzungen darin genügend verankert ist.
2. Die Verantwortlichkeiten innerhalb des DVI betreffend Kontrolle der Einhaltung der Datenschutzvorschriften sind zu klären.

Hinweise:

1. Das DVI hat innert 30 Tagen schriftlich zu erklären, ob es der Empfehlung folgen wird.
2. Die vorliegende Empfehlung wird auf www.ag.ch/idag publiziert.

lic.iur. Gunhilt Kersten
Beauftragte