



DATENSCHUTZ AKTUELL

22. Dezember 2022

(Öffentlichkeits- und)
Datenschutzbeauftragter
Schwyz - Obwalden - Nidwalden

Jahrgang 2022, Ausgabe 2

In dieser Ausgabe:

Editorial	1
Ihre Meinung ist gefragt: Welche Stellen sollen wir kontrollieren?	1
Was macht eigentlich ein Datenschutzbeauftragter mehrerer Kantone so ...?	1/2
Gesichtssuchmaschinen - Die Abschaffung der Anonymität	2/3
„Aus der Praxis“	3/4



Geschätzte Leserinnen
und Leser

Schon wieder neigt sich das Jahr dem Ende zu. Das Thema Datenschutz wurde auch 2022 viel diskutiert.

Am 1. September 2023 werden auf Bundesebene das totalrevidierte Datenschutzgesetz, die ausführende Verordnung sowie weitere Bestimmungen in Kraft treten. Mit neuen Technologien und Möglichkeiten muss immer auch der Datenschutz mitgedacht werden.

Editorial

Die Persönlichkeits- und Freiheitsrechte der Bürgerinnen und Bürger haben respektiert zu werden.

Was gibt es von unserer Seite zu vermelden? Wir informieren zum Europäischen Datenschutzrechtstag und fragen aktiv nach Ihrer Meinung über Kontrollvorschläge.

Ein Artikel zu Gesichtssuchmaschinen macht auf diese illegalen Dienste aufmerksam und rät von der Nutzung derselben strengstens ab. In Europa wurden deswegen bereits Höchststrafen wegen Datenschutzverletzungen verhängt.

Wie immer erhalten Sie mit unseren Praxisfällen einen Einblick in Fragestellungen, die in den Bereichen Datenschutz (SZ/OW/NW) sowie Öffentlichkeitsprinzip (nur SZ) an uns herangetragen wurden.

Wir wünschen Ihnen viel Spass bei der Lektüre unseres Newsletters, frohe Festtage und einen guten Start ins neue Jahr.

Sonja Burkart

Sonja Burkart

Ihre Meinung ist gefragt: Welche Stellen sollen wir kontrollieren?

Im Jahr 2023 wird die Datenschutzstelle der Kantone Schwyz, Obwalden und Nidwalden seit 15 Jahren bestehen. Nicht zuletzt deshalb probieren wir etwas Neues aus: Gerne möchten wir Sie in Teile unsere Tätigkeit mit einbeziehen.

Als Datenschutzbeauftragter der Kantone Schwyz, Obwalden und Nidwalden sind wir gemäss deren drei kantonalen Datenschutzgesetze die Aufsichtsstelle im Bereich der Bearbeitung von Personendaten durch öffentliche Organe. Unsere in diesen Gesetzen verankerten Aufgaben erfüllen wir, indem wir neben der Beratung, Sensibilisierung und Information auch Kontrollen bei

öffentlichen Organen durchführen. Zudem müssen wir geplante Datenbearbeitungen, die besondere Risiken für die Grundrechte der betroffenen Person bergen, vorgängig überprüfen.

Teilen Sie uns mit, welche Stellen Sie aufgrund welcher Begebenheiten, Erfahrungen, Hintergründe oder Ängste (z.B. um die Sicherheit ihrer persönlichen Daten) von uns kontrolliert haben möchten. Es interessiert uns, was Sie interessiert. Wir können Ihnen nicht garantieren, dass wir die uns gemeldeten Stellen auch tatsächlich werden kontrollieren können. Ihre Inputs werden wir aber sorgfältig

prüfen und auswerten. Dabei werden wir evaluieren, ob (und falls ja, wie genau) sich diese in unser Kontroll- bzw. Tätigkeitsprogramm integrieren lassen.

Gerne betonen wir deshalb erneut: Melden Sie sich bei uns und wirken Sie so bei der Erfüllung unseres Auftrags mit. Sagen Sie uns, welche Bereiche Sie interessieren und welche Stellen/Behörden wir hinsichtlich der Bearbeitung von Personendaten in Bezug auf ihren gesetzlichen Auftrag kontrollieren sollen.

Philipp Studer

Was macht eigentlich ein Datenschutzbeauftragter mehrerer Kantone so ...?

In diesem Newsletter verzichte ich explizit auf einen Rückblick zum bald vergangenen Jahr 2022 und auf einen Ausblick auf das kommende Jahr. Dafür lade ich Sie und alle Interessierten auf ein Gespräch mit mir im Rahmen des Europäischen Datenschutzrechtstags ein.

Uns gegenüber stellen sich oft Fragen wie die folgenden:

Wo machen Sie Kontrollen und was bringen diese (konkret) bzw. wie sehen jeweils die Resultate aus? Was tun Sie genau bei Ihrer täglichen Arbeit? Welche Daten schüt-

zen Sie und wie tun Sie das? Wieso sind Sie nicht häufiger vor Ort (z.B. mit Kontrollen)? Was machen sie neben Kontrollen sonst noch?

Auf alle diese, aber auch auf andere Fragen können Sie im Januar ...

Was macht eigentlich ein Datenschutzbeauftragter



Bildquelle: ibs.de



Bildquelle: Toni Hegewald / pixello.de

2023 von mir eine Antwort erhalten. Da die Datenschutzstelle der Kantone Schwyz, Obwalden und Nidwalden im November 2023 seit 15 Jahren bestehen

wird, möchten wir uns gerne mit der Bevölkerung bzw. interessierten Personen austauschen und somit deren «Puls fühlen» können. Wir möchten in Erfahrung bringen, was für die Bevölkerung wichtig ist und wo sie ein Agieren von uns sehen möchte.

Gerne werde ich als (Öffentlichkeits- und) Datenschutzbeauftragter

der Kantone Schwyz, Obwalden und Nidwalden Ihnen und anderen interessierten Personen im Rahmen

„Kommen Sie mit Ihren Anliegen und Fragen zu uns.“

des jeweils Ende Januar stattfindenden Europäischen Datenschutzrechtstag «Red und Antwort» stehen. Bringen Sie Ihre Fragen mit. Ich freue mich auf diese und auf eine rege Diskussion mit am Datenschutz interessierten Personen. Es gibt nämlich viele Themen im Bereich Datenschutz, die man nicht vergessen sollte, weil sie uns alle

etwas angehen (da auch unsere persönlichen Daten davon betroffen sein können).

Bei Interesse an diesem Austausch, der für den Freitag, 27. Januar 2023 geplant ist, melden Sie sich bitte per email bei uns an.

Philipp Studer

Gesichtssuchmaschinen - Die Abschaffung der Anonymität

Gesichtssuchmaschinen können auch das Leben von Personen aus den Kantonen Schwyz, Ob- und Nidwalden berühren. Wir zeigen auf wieso.

Clearview AI

Vor einigen Jahren geriet das US-amerikanische Tech-Unternehmen Clearview AI in die Schlagzeilen. Es filtert ungefragt Gesichter aus dem Internet, wertet diese biometrisch aus, katalogisiert sie und stellt die Daten der Polizei und anderen Strafverfolgungsbehörden zur Verfügung.

PimEyes

Die Computersoftware PimEyes ist hingegen für Private bzw. zahlende Nutzer gedacht. Gemäss PimEyes sollen Menschen herausfinden können, wer ihre Fotos im Netz verbreitet. PimEyes verspricht, dass Personen ein Foto von sich hochladen können, damit diese Fotos nicht mehr in späteren Suchresultaten gefunden würden. Dieser Schutz mit Namen „PROtect“ kostet etwas unter 100 Franken im Monat.

Welche Funktionen haben diese Suchmaschinen?

Es braucht nur einen Screenshot oder ein Foto einer Person, um diese im Netz zu suchen. Die Suchmaschine erfasst die biometrischen Merkmale des Gesichts (z.B. die Abstände von Augen, Nase und Mund). PimEyes findet als Ergebnis ähnliche oder gar identische Gesichter inkl. Link zum Fundort im Internet. Es gibt verschiedene „Nutzungsabos“. Mit dem mehrere

hundert Franken teuren Monats-Abos „Advanced“ kann unlimitiert nach Gesichtern gesucht werden und es sind 500 „Alerts“ (Benachrichtigungen) möglich. Der Suchmodus bei diesem Plan nennt sich „deep search“ (tiefgreifende Suche).

PimEyes betont, dass die Software „nicht für die Überwachung anderer Personen gedacht“ sei. Die oben erwähnten unendlichen Suchmöglichkeiten und die 500 Benachrichtigungen sowie die Privatsphäre zu hohen Kosten („PROtect“) lassen wohl auf etwas anderes schliessen.

Gefahren

Ob auf Demonstrationen, im Spital-Wartezimmer, in den öffentlichen Verkehrsmitteln oder auf der Dating-App: Die Zeit der Anonymität ist vorbei. Personen können mithilfe

(DSGVO) der EU. Demnach ist die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person ohne deren ausdrückliche Einwilligung untersagt.

In der Schweiz (Bund und Kantone) wurden die Datenschutzgesetze noch nicht überall angepasst bzw. sind noch nicht in Kraft. Aber auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) liess am 11.02.2020 verlauten (https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html):

„Auch wenn Gesichtsdaten nicht per se als besonders schützenswert i.S. von Art. 3 Bst. c des Bundesgesetzes über den Datenschutz (DSG) einzustufen sind, stellt die Massenbeschaffung von Gesichtsdaten aus internet-zugänglichen

Alle öffentliche Organe in den Kantonen Schwyz, Obwalden und Nidwalden (z.B. Kantonspolizeien, Migrationsämter, Personalämter) sollen auf den Einsatz von Gesichtssuchmaschinen wie Clearview AI oder PimEyes verzichten

der Software und Fotos derselbigen identifiziert werden, wenn sich entsprechendes Material online befindet. Dies hat nicht «nur» Konsequenzen für die Privatsphäre. Auch der Ruf, die Sicherheit oder sogar das Leben der Betroffenen können auf dem Spiel stehen.

Sind die Dienste legal?

Sowohl PimEyes als auch Clearview AI greifen massiv in die informationelle Selbstbestimmung der Menschen ein. Die Dienste verstossen unter anderem auch gegen Artikel 9 der Datenschutzgrundverordnung

Quellen eine Persönlichkeitsverletzung i.S.v. Art. 12 Abs. 2 Bst. a DSG dar, wenn die damit einhergehende Bearbeitung gegen die Grundsätze der Art. 4, 5 Abs. 1 und 7 Abs. 1 DSG verstösst. Wer ungefragt Gesichtsdaten in Massen beschafft und zu Zwecken bearbeitet, die bei der Beschaffung weder deklariert, noch aus den Umständen ersichtlich oder gesetzlich vorgesehen sind, verstösst gegen die Grundsätze der Transparenz, Verhältnismässigkeit und der Zweckbindung.“ ...

„Unsere Privatsphäre wird an verschiedenen Fronten angegriffen.“

© Tim Cook (*01. Nov. 1960)
CEO Apple

Advanced
CHF 317.99/mo

Monthly plan

- ✓ One-month access
- ✓ **Unlimited** searches
- ✓ Access to sources of results (websites and images)
- ✓ Up to **500** PimEyes' Alerts
- ✓ Dedicated support

PROtect + Advanced features:

- ✓ **Deep Search** (more thorough search)
- ✓ PDF and CSV results exporting

Bildquelle: pimeyes.com

Verfahren beim EDÖB und bei EU-Datenschutzbehörden

Aktuell sind sowohl beim EDÖB als auch bei verschiedenen Datenschutzbehörden der EU Massnahmen getroffen worden (z.B. Auskunfts- und Löschgesuche). Auch Verfahren gegen einen oder beide Dienste sind in verschiedenen Ländern hängig oder bereits abgeschlossen. So hat die französische Datenschutzbehörde CNIL im Oktober 2022 Clearview AI mit der in der DSGVO vorgesehenen Höchststrafe (!) von 20 Millionen Euro gebüsst (<https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai>). Die Gesichtsbilder dürfen zudem nicht mehr illegal verwendet werden und müssen gelöscht werden.

Kein Einsatz dieser Gesichtserkennung

Der EDÖB rät ab «Abgleiche mit Gesichtsbildern ohne Einwilligung

der Betroffenen vorzunehmen“ und ist deswegen unter anderem an die Strafverfolgungsbehörden des Bundes gelangt.

Im März 2020 wurde bestätigt, dass die Direktionen des Bundesamts für Polizei, das Bundesamt für Zoll und Grenzsicherheit sowie der Nachrichtendienst des Bundes „in ihrer Tätigkeit Software wie Clearview weder einsetzen noch einzusetzen beabsichtigen“.

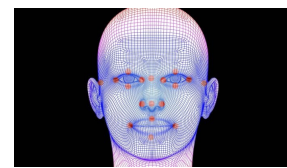
Unsere Empfehlung für SZ/OW/NW

Wir vertreten in unserem Tätigkeitsgebiet die Sichtweise des EDÖB und der europäischen Datenschutzbehörden und empfehlen darum jeglichen öffentlichen Organen (z.B. Kantonspolizeien, Migrationsämtern, Personalämtern) auf den Einsatz von solchen oben beschriebenen Softwares zu verzichten.

Zudem dürfen öffentliche Organe

grundsätzlich nur mit (freiwilliger und einzelfallbezogener) Einwilligung der betroffenen Personen Fotos auf Homepages oder in anderen Publikationen veröffentlichen. Das „Recht am eigenen Bild“ muss eingehalten werden. Personen dürfen keine Nachteile (oder weniger Vorteile) erfahren, wenn sie mit einer Veröffentlichung nicht einverstanden sind. Öffentliche Organe sind zudem weiterhin angehalten, das Bildmaterial mit technischen und organisatorischen Massnahmen gegen unbefugte Bearbeitung (also auch solcher) zu schützen.

Sonja Bukart



Bildquelle: imago / Science Photo Library

„Aus der Praxis“

+ Muss ich das E-Mail, das ich einem Mitarbeitenden eines anderen Amtes geschrieben habe aufgrund des Öffentlichkeitsprinzips einem (an diesem Vorgang unbeteiligten) Dritten herausgeben?

Solche oder ähnliche Anfragen erhalten wir viele; und zwar von öffentlichen Organen wie auch von interessierten Privaten. Dabei erklären wir jeweils das Vorgehen im Bereich Öffentlichkeitsprinzip wie folgt:

Es geht darum, die Abklärungen betreffend einer eventuellen Herausgabe amtlicher Dokumente in zwei Schritten vorzunehmen. Als erstes ist abzuklären, ob das betreffende / erfragte Dokument (E-Mail, Studie, Brief, etc.) ein amtliches Dokument darstellt. Dazu ist festzu-

halten, dass nach § 4 Bst. b ÖDSG amtliche Dokumente als Aufzeichnungen definiert werden, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von der Darstellungsform und vom Informationsträger. Ausgenommen sind Aufzeichnungen, die nicht fertig gestellt (z.B. Skizzen oder Entwürfe) oder ausschliessen für den persönlichen Gebrauch bestimmt sind (z.B. Handnotizen). Stellt das verlangte Dokument kein amtliches Dokument dar, muss es nicht gemäss Öffentlichkeitsprinzip herausgegeben werden und weitere diesbezügliche Abklärungen erübrigen sich.

Erst im zweiten Schritt (und nur wenn ein amtliches Dokument vorliegt) wird eruiert, ob das oder die

verlangte/n amtliche/n Dokument/e herausgegeben werden müssen. Nun ist abzuklären, ob eine Ausnahmebestimmung nach § 6 ÖDSG vorliegt. Falls nein, darf das Dokument herausgegeben werden. Falls eine Ausnahme vorliegt, darf das amtliche Dokument entweder überhaupt nicht oder nur teilweise oder erst zu einem späteren Zeitpunkt herausgegeben werden.

Im konkreten Fall musste die E-Mail aufgrund überwiegender privater Interessen, die darin in grosser Menge enthalten waren, nicht herausgegeben werden.

DSB SZ-OW-NW

+ Dürfen für den Schaltdienst kurze und einfache Gruppenpasswörter verwendet werden?

Ein öffentliches Organ fragte bei uns an, ob für den Schaltdienst ein einfaches und kurzes Gruppenpasswort verwendet werden darf. Dieses könnten alle Mitarbeitenden miteinander teilen. So müsste die Kundschaft am Schalter nicht «lange» warten, bis das persönliche Passwort eingegeben worden sei.

Die Antwort zur Frage ist eindeutig. Jeder Nutzer muss ein eigenes und

zudem sicheres Passwort verwenden. Kurze und einfache Gruppenpasswörter sind nicht zulässig.

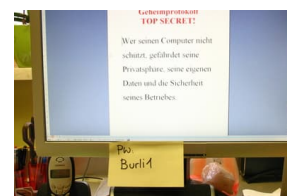
Passwörter sind der wohl grösste Risikofaktor der IT-Sicherheit. 63 Prozent aller Datendiebstähle sind gemäss dem diesjährigen «Data Breach Investigations Report» des Telekommunikationskonzerns Verizon auf unsichere oder gestohlene Passwörter zurückzuführen. Das Passwort darf also nicht zu kurz und einfach sein. Meist gibt es Passwortrichtlinien von den IT-Verantwortlichen, die auf den neu-

esten Sicherheitsstandards beruhen sollten. Verwendet man beispielsweise ein langes aber weniger komplexes Passwort mit mindestens 25 Zeichen und nur zwei Zeichenarten (z.B. Gross- und Kleinbuchstaben) ist dies gemäss dem Bundesamt für Sicherheit in der Informationstechnik gleich sicher wie ein kürzeres und komplexes Passwort mit mindestens 8 Zeichen und vier Zeichenarten (Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen).

Auf www.passwortcheck.ch kann beispielsweise die Sicherheit ...

„Mit dem Öffentlichkeitsprinzip wurde die Geheimhaltung zur Ausnahme und das Einsichtsrecht zur Regel.“

© www.sz.ch



Bildquelle: Gabi Eder / pixelio.de

„Denken im
Computerzeit-
alter. Er wollte
seinen Verstand
gebrauchen und
hatte das
Passwort
vergessen.“

© Siegfried Wache (*1951),
technischer Zeichner,
Luftfahrzeugtechniker und
Buchautor



Bildquelle: angieconscious /
pixello.de

eines Passwortes überprüft werden. Zudem wird die Rechenzeit zur Ermittlung des Passwortes geschätzt. Diese beträgt beispielsweise beim (im Privatgebrauch) am meisten verwendeten Passwort «123456» weniger als eine Sekunde. Tipp von uns: beim Testen auf der Plattform NICHT das Originalpasswort verwenden.

Passwörter müssen immer persönlich sein und dürfen nirgends auf-



Warum sind nicht alle Halter von Fahrzeugen im Kanton Nidwalden auffindbar?

Eine Person wollte aus Neugierde wissen, wem ein Nidwaldner Kontrollschild gehört und suchte nach der entsprechenden Nummer. Als sie diese nicht fand und beim kantonalen Verkehrssicherheitszentrum keine Auskunft erhielt, meldete sie sich bei uns.

Früher gab es ein grosses Buch mit allen Nummern (Autoindex). Diesen Autoindex konnte jedermann bestellen. Darin waren die Autonummern sowie die dazugehörigen Halter (numerisch geordnet) aufgelistet. Die anfragende Person wollte wissen, warum die Suche nicht mehr uneingeschränkt möglich ist.

Der Grund lässt sich auf die Digitalisierung zurückführen. Sobald der

Autoindex als durchsuchbares PDF elektronisch verfügbar war, wurden auch Abfragen nach Personen möglich. So konnte nicht mehr nur nach Nummern, sondern auch konkret nach Haltern und ihren Autonummern gesucht werden. Mit der Zeit wurde der Wunsch nach Privatsphäre und Datenschutz lauter (z.B. vermehrte Werbung, aufdringliche Personen, Neugierde).

So ist es heute in der ganzen Schweiz möglich, die Halterdaten per Gesuch beim zuständigen kantonalen Strassenverkehrsamt gebührenfrei sperren zu lassen. Dies wird in Art. 89 g Abs. 5 des Strassenverkehrsgesetzes (SVG, SR 741.01) geregelt. Ein Halter muss also selbst aktiv werden, um seine Daten zu sperren. Ein Grund für die Sperrung muss nicht angegeben werden. Das Recht gilt voraussetzungslos. Das Verkehrssicherheits-

zentrum und vielleicht auch «schätzen». Diese zeigt nämlich, dass sich das öffentliche Organ an die Datenschutz- und IT-Sicherheitsstandards hält und mit den Angaben aller Einwohnenden sorgfältig umzugehen weiss.

DSB SZ-OW-NW

zentrum bietet auf seiner Webseite ein Formular zur einfachen und schnellen Sperrung an.

Die Datenweitergabe an private Organisationen und Personen erfolgt bei gesperrten Daten nur im Hinblick auf die Bekanntgabe der Namen von Fahrzeughaltern und ihrer Versicherer bei Unfällen, Halterwechsel gegenüber dem neuen Halter und falls im Hinblick auf ein Verfahren ein hinreichendes Interesse geltend gemacht werden kann. Halter können sich also in solchen Fällen nicht «hinter dem Datenschutz verstecken».

DSB SZ-OW-NW



(Öffentlichkeits- und) Datenschutzbeauftragter
Schwyz - Obwalden - Nidwalden

Gotthardstrasse 21
6414 Oberarth

Telefon 041 859 16 20
Fax 041 859 16 26
E-Mail: info@kdsb.ch
www.kdsb.ch