DATENSCHUTZ AKTUELL

18. Dezember 2019

(Öffentlichkeits- und)
Datenschutzbeauftragter
Schwyz - Obwalden - Nidwalden

Jahrgang 2019, Ausgabe 2

Editorial

Sie halten unseren zweiten Newsletter für dieses Jahr in den Händen oder lesen diesen online. Was erwartet Sie?

Im ersten Artikel schauen wir passend zum Jahresende zurück auf das vergangene Jahr unserer Tätigkeit und versuchen bereits jetzt, einige Schwerpunkte für das kommende Jahr zu setzen.

Der zweite Artikel befasst sich mit Multifunktionsgeräten. Diese sind heute keine «einfachen» Kopierer oder Drucker mehr, sondern beherbergen viele Daten, die geschützt werden müssen. Wir geben Ihnen darüber einige Informationen und Tipps.

Die kantonsspezifischen „Aus der Praxis"-Fälle behandeln im Kanton Schwyz die Frage, was mit Zugangsgesuchen betreffend Öffentlichkeitsprinzip passiert, wenn diese nicht an die zuständige Instanz gesendet werden. Im Kanton Obwalden geht es um die Bekanntgabe von Personendaten im Zusammenhang mit Vereinsbeiträgen. In Nidwalden waren Fotofallen zur Wildbeobachtung ein Thema, weil diese auch menschliche Waldbesucher/innen erfassen können.

Besten Dank für Ihr Interesse am Datenschutz, dem Öffentlichkeitsprinzip und an unserer Arbeit. Wir wünschen Ihnen viel Spass bei der Lektüre und frohe Festtage.

Sonja Burkart

Hier können Sie unsere News (u. a. „DATENSCHUTZ AKTUELL") abonnieren:
http://www.kdsb.ch/xml_1/internet/de/application/d12/f17.cfm

In dieser Ausgabe:

Bildquelle: www.flickr.com

2019 vs. 2020

Im Jahr 2019 erreichten uns erneut sehr viele Anfragen. Daneben führten wir Kontrollen durch, prüften einige Gesetzesvorlagen und sensibilisierten verschiedene Stellen und Personen (z.B. an Schulungen). Für unsere Arbeiten im Jahr 2020 werden wir im Januar das Tätigkeitsprogramm festlegen.

Als (Öffentlichkeits- und) Datenschutzbeauftragter der Kantone Schwyz, Obwalden und Nidwalden (ÖDB) erfüllen wir unterschiedlichste Aufgaben. Zu diesen gehören unter anderem: Kontrolle öffentlicher Organe; Beratung öffentlicher Organe und Privater; Prüfen von Gesetzgebungsvorhaben; Sensibilisierung von Behörden, Stellen und oft auch Privaten (z.B. mit Kursen & Referaten) und Information der Bevölkerung. Letzteres geschieht v.a. per Tätigkeitsbericht, Newsletter und Webseite.

Was war 2019?

Gerne schauen wir auf das ausklingende Jahr 2019 zurück. Ausführlicher tun wir dies jeweils in unserem Tätigkeitsbericht, über den wir nach dessen Kenntnisnahme durch unsere Aufsichtsorgane informieren werden.

2019 führten wir einige kleinere *Kontrollen* zu verschiedenen Teilaspekten des Datenschutzes bei öffentlichen Organen durch. Daneben gingen bei uns einige Meldungen zu möglichen Verfehlungen vor Ort ein, die wir im Rahmen der uns zur Verfügung stehenden Ressourcen (meist nicht vor Ort) überprüften oder noch überprüfen werden. Weiter erstellten wir die Berichte zu den Kontrollen der Nutzung des Schengener Informationssystems bei den Kantonspolizeien Obwalden und Nidwalden, die im Vorjahr stattfanden.

Datenschutz und Öffentlichkeitsprinzip werden immer wichtiger (erst recht in unserer verknüpften Welt). Das zeigt sich in der Praxis, indem immer mehr Personen und Stellen mit ihren Fragen an uns gelangen.

Zudem kontrollierten wir die Umsetzung der Pendenzen, die wir in den Kommunaluntersuchen und Datenschutzreviews bei Gemeinden und Bezirken (aller Vereinbarungskantone) während der Legislatur 2012-2016 ausgewiesen hatten. Dabei wurde auch der Umgang und die Sensibilisierung im Bereich Datenschutz an den Schulen untersucht. Diese Pendenzenkontrolle verursachte 2019 viel Aufwand und wird es wohl auch 2020 noch tun.

Es erreichten uns 2019 erneut sehr viele *Anfragen* zu oft auch komplexen und/oder heiklen Themen. Deshalb beanspruchte deren Beantwortung oft längere Zeit und wir mussten gewisse anfragende Personen und Stellen vorerst vertrösten, bis wir uns um deren Anliegen kümmern konnten. So waren beispielsweise die Videokameras noch immer aktuell. Daneben scheint der Datenschutz vielen Personen in ihrem persönlichen und dem Arbeitsumfeld immer wichtiger zu werden. Das freut uns, fordert uns aufgrund der vielen Fragen immer wieder heraus.

Neben der Revision der kantonalen Datenschutzgesetze beschäftigte uns bei der *Gesetzgebung* auch einige neue Vorlagen der Kantone und des Bundes, zu denen wir uns entsprechend geäussert haben. Dabei geht es oft auch darum, dass man den Angaben der Bürgerinnen und Bürger angemessen umgegangen wird. ...

Bildquelle: kalenderpedia.de

2019 sensibilisierten wir an unseren *Kursen* zum Datenschutz (in SZ, OW und NW) und zum Öffentlichkeitsprinzip (nur in SZ) Mitarbeitende verschiedener öffentlicher Organe. Weiter fanden spezifische Kurse zum Datenschutz für Lehrpersonen (v.a. OW), für Lernende der Kantonsverwaltung (SZ) und für Rechtspraktikanten der Zentralschweiz statt. Zudem referierte der ÖDB bei der Kantonspolizei OW zum Umgang mit dem Schengener Informationssystem.

In diesem Jahr beantworteten wir verschiedene Medienanfragen und gaben zwei Newsletter heraus. Zudem stellten wir die neue Rubrik «Ihre Rechte» auf unserer Webseite online. Diese dient Bürgerinnen und Bürgern dazu, ihre Rechte gegenüber Behörden und Amtsstellen geltend machen zu können (z.B. Haltersperre, Datensperre).

Was geschieht 2020?

Neben der fortzuführenden Pendenzenkontrolle bei Gemeinden, Bezirken und Schulen planen wir für 2020 bereits gewisse *Kontrollen*. Näheres dazu werden Sie im Tätigkeitsbericht 2020 erfahren. Zudem wollen wir noch genügend Zeit haben, um Meldungen untersuchen und entsprechend handeln zu können.

Die *Beratung* öffentlicher Organe und Privater wird auch 2020 einen wichtigen Teil unserer Arbeit darstellen. Wir werden – trotz bereits bestehender grösserer Anfragen – versuchen, eine möglichst zeitnahe Beratung anzubieten. Wichtig ist dabei vor allem, dass die öffentlichen Organe korrekt mit den Angaben der Bürgerinnen und Bürger umgehen.

Im Bereich der *Gesetzgebung* wird uns die Revision der Datenschutzgesetze der Kantone Ob- und Nidwalden beschäftigen. Zudem steht in beiden Kantonen eine Diskussion zur Umsetzung des Öffentlichkeitsprinzips an, wo wir uns ebenfalls einbringen werden. Weiter werden bestimmt wieder mehrere Vorlagen zur Prüfung zu uns gelangen.

Für 2020 planen wir erneut unsere Grundkurse zum Datenschutz (SZ, OW und NW) und zum Öffentlichkeitsprinzip (nur SZ). Daneben werden eine Schulung für die Lehrpersonen in Obwalden, eine für die Lernenden der Kantonsverwaltung Schwyz sowie spezifische Kurse für eine Schule und eine Gemeinde stattfinden. Weiter wurde der ÖDB bereits für ein Referat angefragt.

2020 planen wir die Herausgabe von zwei Newslettern und werden den Medien im Rahmen unserer Ressourcen bei Fragen in unserem Zuständigkeitsbereich gerne Auskunft erteilen.

Fazit

Datenschutz und Öffentlichkeitsprinzip werden in der Praxis öffentlicher Organe und auch für Private immer wichtiger. Dabei versuchen wir fortwährend, den öffentlichen Organen zu helfen, die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger zu wahren und im Rahmen des Öffentlichkeitsprinzips mögliche Auskünfte erteilen zu können.

Philipp Studer

„Nicht einmal im Rückblick wird alles vorhersagbar."

© Ernst Ferstl (*1955), österr. Lehrer, Dichter und Aporistiker

Sicherheitslücke Multifunktionsgerät?

Gerade in Grossraumbüros sind sie kaum mehr aus dem Alltag wegzudenken: Multifunktionsgeräte. Diese sind für ganze Teams im Einsatz und beeindrucken mit vielfältigen Funktionen. Sie können unter anderem drucken, scannen, faxen, mailen und kopieren.

Dass ein Multifunktionsgerät Datenschutz- und Datensicherheitsrisiken beherbergen kann, sind sich viele Leute nicht bewusst. Hier zeigen wir einige Risiken und damit verbundene Strategien auf, diesen zu begegnen.

Weitreichende Personendatenspeicherungen

Mithilfe der Multifunktionsgeräte finden täglich vielfältige Bearbeitungen von Personendaten statt. Bewerbungsunterlagen und Personalbeurteilungen, Lohnabrechnungen, Fotos, medizinische Berichte und Gutachten, Asylanträge, Unterlagen zu Straf- und Verwaltungsverfahren usw. werden gedruckt, gescannt oder sonstwie an Multifunktionsgeräten bearbeitet.

Diese speichern funktionsbedingt riesige Datenmengen an Informationen. Mit ein wenig Know-How können diese Informationen abgesogen und missbraucht werden. Damit ergibt sich ein grösseres Sicherheitsrisiko als z.B. beim altbekanntem Risiko vom Vergessen eines heiklen Aktenstücks im Kopierer oder Drucker.

Zugangsbeschränkung und Schutzmassnahmen

Zum Teil finden sich Geräte gut zugänglich und unbeaufsichtigt im Gang und ganze Teams haben darauf Zugriff. Unter Umständen könnten sich theoretisch auch Fremde zu solchen Informationen Zugang verschaffen. Dies ist durch entsprechende Zugangskontrollen bzw. Passwörter und Beaufsichtigung von Gästen oder unbefugten Personen zu verhindern.

Auch innerhalb von Teams sollten Druckerzugänge möglichst funktionsbezogen erfolgen. So sollte z.B. das Personalamt über ein anderes Multifunktionsgerät verfügen als das Bauamt und die Zugänge dazu geregelt werden. Datenschutz und Datensicherheit sollen auch in diesem Bereich gelten und es soll verhindert werden, dass Personendaten an Leute gelangen, welche diese nicht bearbeiten dürfen.

So empfehlen sich je nach Schutzstufe der Daten (z.B. besonders schützenswerte Personendaten) bzw. der Aufgabengebiete der Mitarbeitenden allenfalls spezielle Geräte, Kopierkarten, Schlüssel oder Freigabecodes.

Geschützter Druck in Einzelfällen

Werden sensible Informationen gedruckt, empfiehlt sich die Aktivierung einer Funktion, welche für diesen Druckauftrag einen geschützten Druck erlaubt. Die Funktion lässt sich meist im Druckmanager einschalten. Nach der Aktivierung werden abgesendete Druckaufträge erst ausgedruckt, wenn am Multifunktionsgerät ein Passwort eingegeben wird. So kann verhindert werden, dass andere Personen die Ausdrucke sehen.

Eigenverantwortung und Schulung

Die Nutzenden können darauf achten, einander nicht dazwischen sondern möglichst nacheinander zu drucken. Dies erleichtert auch das Auffinden der eigenen Dokumente bzw. den Zeitaufwand dafür. Zudem sollte man – wie auch bei einem normalen Kopierer – darauf achten, keine Originale oder Ausdrucke zu vergessen. Alle Unterlagen sollten möglichst sofort vom Gerät an den Arbeitsplatz geholt werden. Fehldrucke mit Personendaten sollten sofort geschreddert bzw. speziell entsorgt werden.

Heikle Scans sollten allenfalls verschlüsselt abgelegt werden oder sich verschlüsselt an einen gespeicherten Adressbucheintrag (keine Tippfehler) schicken lassen. ...

Screenshot zu geschütztem Druck

Wird ein Scan in ein allgemeines Teamlaufwerk abgelegt, soll dieser danach sofort korrekt beschriftet und in den passenden Arbeitsordner abgelegt werden.

Am besten sind entsprechende, bereichs- und sicherheitsspezifische Regelungen für alle Mitarbeitenden bzw. Teams, die heikle Daten bearbeiten, zu erlassen und die betreffenden Personen über diese Regelungen zu schulen.

Multifunktionsgeräte müssen so betrieben werden, dass keine Informationen (Ausdrucke, Scans, Daten des Speichers usw.) an Unbefugte gelangen können.

Kontrolle von Diensten und Passwörtern

Für nahezu jedes Gerät sind entsprechende Zugangsdaten verfügbar (Handbücher, Internet, usw.): Standardpasswörter, Codes für Administratoren oder Tastenkombinationen, die beim Einschalten des jeweiligen Geräts gedrückt werden müssen. Werden diese bei Inbetriebnahme nicht geändert, lassen sich von Unbefugten leicht administrative und somit allumfassende Rechte für den Zugang zum Innersten der Kopiersysteme zu erhalten. Deshalb empfiehlt es sich, alle Codes abzuändern (sichere Codes bzw. Passwörter).

Sollen Dienste, Zusatzmodule und Netzwerkverbindungen nicht (oft) benötigt werden, empfiehlt es sich, diese standardmässig auszuschalten. So besteht kein Zugriff bzw. muss dieser erst aktiviert werden. Je weniger Verbindungen bestehen, desto weniger angreifbar ist das Gerät.

Technik und Wartung

Bei Lieferung ist ein Geräteabnahmeprotokoll zu verlangen und durchzuarbeiten, um sicherzustellen, dass sicherheitsrelevante Einstellungen nach Vorgabe konfiguriert sind.

Sicherheitsupdates, die von den Herstellern zur Verfügung gestellt werden, sollten umgehend installiert werden, um bekannte Sicherheitslücken im Kopiersystem zu schliessen. Dies gilt insbesondere dann, wenn der Kopierer als Multifunktionsgerät innerhalb eines Computernetzwerks betrieben wird.

Im Rahmen der Technik/Wartung soll die Funktionsfähigkeit der Systems garantiert werden bzw. die entsprechenden Einstellungen dazu gemacht werden können. Nach Möglichkeit sollten nur Systeme angeschafft werden, bei denen es möglich ist, die Daten innerhalb des Systems vor dem Wartungszugriff zu schützen. Mit Lieferanten und Wartungsfirmen sind entsprechende Geheimhaltungspflichten zu vereinbaren, wenn umfassende Zugriffe auf Personendaten und nicht nur Einstellungen möglich sind.

Hacking ist möglich!

Unbefugte können sich mit den entsprechenden Passwörtern (siehe oben) leicht Zugang zu noch vorhandenen Daten alter Kopien, Faxe oder Druckaufträge verschaffen.

Ist das Multifunktionsgerät mit einem lokalen Computer-Netzwerk verbunden, können sachkundige Hacker sich von einem beliebigen Gerät des Netzwerks Zugang zu den gespeicherten Daten der Geräte verschaffen. Ist Fernzugriff auf das Netz möglich, ist der Zugriff auch von aussen möglich.

Es empfiehlt sich, separate Netzwerkzonen für Drucker, Kopierer und Multifunktionsgeräte zu verwenden und sicherzustellen, dass diese und alle entsprechenden Geräte bei Sicherheitsprüfungen überprüft werden.

Datenvernichtung

Nicht mehr auf dem Gerät ersichtliche oder vermeintlich gelöschte Angaben lassen sich mit geringem technischen Aufwand wiederherstellen. Die notwendigen Informationen hierzu sind im Internet zu finden.

Deshalb gilt:

Werden Geräte entsorgt, weitergegeben oder zurückgegeben, müssen alle Daten, die noch auf dem System verblieben sind, fachmännisch gelöscht werden. Falls dies nicht wirksam erreicht werden kann, müssen die Datenträger – genau wie PC-Festplatten – physisch zerstört werden.

Sonja Burkart

Bildquelle: store.xerox.eu

„Sicher ist, dass nichts sicher ist, selbst das nicht."

© Joachim Ringelnatz (1883-1934), eigentl. Hans Bötticher, dt. Lyriker, Erzähler und Maler

„Aus der Praxis"

Was geschieht, wenn eine Person ihr Gesuch um Zugang zu (einem) bestimmten amtlichen Dokument(en) bei einer nicht dafür zuständigen Behörde/Stelle einreicht?

Nach § 5 Abs. 1 des Gesetzes über die Öffentlichkeit der Verwaltung und den Datenschutz des Kantons Schwyz (ÖDSG) hat jede Person Anspruch darauf, amtliche Dokumente einzusehen und Auskunft über den Inhalt amtlicher Dokumente zu erhalten.

Wer Einsicht in ein amtliches Dokument oder Auskunft über dessen Inhalt verlangt, richtet ein Gesuch im Sinne von § 32 an das öffentliche Organ, welches das betreffende Dokument besitzt (§ 7 Abs. 1 ÖDSG). Dieses Gesuch muss gemäss § 7 Abs. 2 ÖDSG nicht begründet werden, aber die für die Identifizierung des gesuchten Dokuments notwendigen Angaben enthalten. Das öffentliche Organ muss wissen, welches bzw. welche Dokumente eingesehen werden wollen.

Gemäss §§ 7 Abs. 1 und 27 Abs. 1 ÖDSG ist für die Gewährung des Zugangs zu amtlichen Dokumenten das öffentliche Organ zuständig, das im Besitz des betreffenden Dokuments ist.

Die regierungsrätliche Verordnung zum Öffentlichkeits- und Datenschutzgesetz (VÖDSG) enthält auch Ausführungsbestimmungen zum Öffentlichkeitsprinzip. So legt § 5 VÖDSG Genaueres zum Gesuch fest. Dabei legt § 5 Abs. 3 VÖDSG eine Nachfrist von zehn Tagen fest, die das öffentliche Organ dem Gesuchsteller ansetzen kann, wenn die Angaben zur Identifizierung des gewünschten Dokuments nicht ausreichen.

Gemäss § 6 Abs. 1 VÖDSG prüft das öffentliche Organ, das um Auskunft über den Inhalt eines amtlichen Dokuments oder um Einsichtnahme in ein solches ersucht wird, seine Zuständigkeit. Wird sie verneint, ist das Gesuch an die zuständige Stelle weiterzuleiten. Sind nach Massgabe von § 27 Abs. 1 ÖDSG mehrere öffentliche Organe zuständig ist das Gesuch von jenem öffentlichen Organ zu behandeln, welches das Dokument erstellt hat.

Zusammengefasst muss das unzuständige öffentliche Organ ein bei ihm eingegangenes Gesuch dem zuständigen öffentlichen Organ weiterleiten und darf dieses nicht wegen Unzuständigkeit abweisen.

DSB SZ-OW-NW

Bildquelle: www.adv.aero

„Wie fruchtbar ist der kleinste Kreis, wenn man ihn wohl zu pflegen weiss.“

© Johann Wolfgang von Goethe (1749-1832), gilt als der bedeutendsten Repräsentanten deutschsprachiger Dichtung

Müssen Vereine Mitgliederlisten abgeben, um Förderungsbeiträge zu erhalten?

Förderungsbeiträge sind oft von der Grösse eines Vereins abhängig. So werden Vereine oft erst ab einer Mindestanzahl von Mitgliedern gefördert. Beiträge können zudem mit der Grösse des Vereins in einem Zusammenhang stehen. So erhalten Vereine mit mehr Mitgliedern oftmals höhere Förderungsbeiträge als solche mit weniger Mitgliedern.

Darum stellt sich die Frage, ob es ausreicht, nur die Anzahl der Vereinsmitglieder anzugeben oder ob der Verein dem Gesuch um Förderbeiträge die ganze Mitgliederliste beilegen muss und somit für die zuständige Stelle ersichtlich wird, welche Personen Mitglieder des Vereins sind.

Der Unterstützungsbeitrag für Vereine hängt von der Anzahl der Mitglieder ab, nicht jedoch davon, wer genau diese Mitglieder sind. Deshalb reicht es aus, nur die Anzahl der Mitglieder an einem gewissen Stichtag anzugeben. Eine Personendatenbearbeitung im Rahmen der Förderungsbeiträge ist also nicht vorgesehen. Die entsprechenden Formulare der öffentlichen Organe, welche Vereine fördern, müssen dies deutlich zum Ausdruck bringen.

Ein Passus, der die Verantwortlichen des Vereins dazu ermahnt, korrekte Angaben zu machen, ist jedoch von Vorteil. So können den Verantwortlichen mögliche Konsequenzen von Falschangaben aufgezeigt werden. Diese können die Rückzahlung sämtlicher ausgerichteter Unterstützungsleistungen beinhalten. Falsche Aussagen können sogar eine Strafanzeige (Betrug, Urkundenfälschung etc.) nach sich ziehen.

DSB SZ-OW-NW

Dürfen Fotofallen für ein Monitoring gewisser Tierpopulationen (z.B. Hirsche oder Luchse) installiert werden?

Mit Fotofallen kann das Leben gewisser Tierarten genauer beobachtet werden. Sie erstellen Fotos, wenn sich gewisse Bewegungen in ihrem vordefinierten Sichtfeld abspielen. Zeichnen Fotofallen Daten auf, auf denen Personen erkennbar sind, wird mit dieser Datenbearbeitung in das Grundrecht auf persönliche Freiheit bzw. in die Privatsphäre dieser Personen eingegriffen. Das Gesetz über den Datenschutz des Kantons Nidwalden (kDSG) dient dem Schutz dieser Privatsphäre. Es legt die Voraussetzungen für das Bearbeiten von Personendaten fest und regelt u.a. auch den Umgang mit Aufnahmen von Videokameras (Art. 17 kDSG). Eingriffe in die Privatsphäre müssen sich auf eine rechtliche Grundlage abstützen und verhältnismässig sein.

Bildquelle: magazin.swisscom.ch

Einzig Fotofallen, die nicht auf Personen, sondern auf Geschehnisse an Örtlichkeiten oder auf reine Objekte ausgerichtet sind und bei denen keine Personen erkennbar sind, beinhalten keine Personendaten. Sie fallen nicht unter den Geltungsbereich des kDSG. Nach Obligationenrecht besteht ein grundsätzliches Betretungsrecht für den Wald. Das Passieren einer Fotofalle von Personen und eine nachfolgende Identifizierung können daher kaum vollständig ausgeschlossen werden.

Der Betrieb von Fotofallen ist datenschutzkonform, wenn folgende Voraussetzungen eingehalten werden:

- Fotofallen dürfen nicht an öffentlichen Plätzen, entlang von Spazier- und Wanderwegen oder an viel begangenen Orten, sondern nur an Kirrungen, Ablenkfütterungen, Fuchs-/Dachsbauten, Wildwechseln etc. betrieben werden.
- Aufnahmegeräte und Standorte müssen signalisiert sein. Auf Hinweisschildern ist der Zweck der Fotofalle anzugeben (z.B. «Überwachung der Wildtierbestände», «Erforschung der Lebensgewohnheiten von Wildtieren» o.ä.).
- Fotofallen müssen eine Kontakt-Adresse des Betreibers enthalten (Name, Vorname, Organisation & Telefon-Nr.).
- Sämtliche Personenaufnahmen (auch Teilaufnahmen bzw. Kleidungsstücke, die auf eine Person zurückschliessen lassen) müssen sofort gelöscht werden.
- Die Weiterverwertung solcher Personendaten (z.B. Speichern oder Weiterleiten) ist verboten.
- Wildkameras und integrierte Speichermedien sind soweit möglich gegen Diebstahl und Vandalismus zu sichern (Datensicherheit).

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