Umfrage zum Thema Datenschutz

Im Jahr 2019 wurde bei der Gemeinschaft der Unterzeichnenden der Charta zur Digitalisierung der Schweizer Land- und Ernährungswirtschaft eine elektronische Umfrage durchgeführt, um Fragen aus der Branche zum Thema Datenschutz zu sammeln. Die 20 dabei eingegangenen Fragen wurden von Ueli Buri, dem Datenschutzbeauftragten des Kantons Bern, wie folgt beantwortet:

1. Daten in der Cloud – Serverstandort in der Schweiz zwingend? Wie ist der Stand der Microsoft-Schweiz-Cloud?

Die Übergabe von Personendaten an Dritte zur Bearbeitung und/oder Aufbewahrung in einer Cloud ist mit verschiedenen Risiken verbunden. Deshalb verbieten die Datenschutzgesetze des Bundes (für Bundesbehörden und private Unternehmen) und der Kantone (für kantonale Behörden) die Bekanntgabe von Personendaten in Länder, in denen kein angemessenes Datenschutzrecht gilt. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) führt eine Liste mit dem weltweiten Stand des Datenschutzes. Das Datenschutzrecht der EU ist zurzeit strenger als jenes der Schweiz, deshalb ist ein Serverstandort in der EU zulässig. Gemäss Ankündigung von Microsoft sollen erste Dienste aus Schweizer Datenzentren noch in diesem Jahr verfügbar sein. Mit Blick auf jedes Outsourcing von Datenbearbeitungen ist zu beachten, dass der Beauftragte (hier der Anbieter von Cloud-Diensten) die Datensicherheit gewährleisten muss und der Weitergabe der Daten keine Geheimhaltungspflicht entgegenstehen darf. Eine solche gilt namentlich für Berufspersonen mit besonderer Vertrauensstellung (Geistliche, Anwälte und Gesundheitsfachpersonen).

2. Was muss ein Landwirt / KMU berücksichtigen, wenn er eine eigene Webseite betreibt?

Falls Personendaten bearbeitet werden (was nicht immer der Fall sein muss), stehen zwei Bearbeitungsformen im Vordergrund: (1) Beobachten und Auswerten des Benutzerverhaltens auf der Website mittels technischer Analysetools. (2) Die Website enthält Felder/Formulare, in denen die Benutzer Personendaten eingeben können, um z.B. einen Newsletter/Informationsmaterial oder direkt eine Leistung zu bestellen (Online-Shop). In beiden Fällen ist in einer verständlichen Datenschutzerklärung darüber zu informieren, welche Daten zu welchem Zweck bearbeitet und gegebenenfalls an welche Dritte (z.B. Bezahldienst) weitergegeben werden sowie an wen sich betroffene Personen wenden können, um ihre Rechte geltend zu machen. Falls eine Datenbearbeitung die ausdrückliche Zustimmung der betroffenen Person erfordert (z.B. Einsatz von Webtracking zur Erstellung von Besucherprofilen), muss diese *vorgängig* – z.B. durch ein gut sichtbares Banner, auf dem die Datenschutzerklärung verlinkt ist und ein Feld «Einverstanden» angeklickt werden muss – eingeholt werden. Alle Personendaten sind gegen unbefugten Zugriff durch Dritte zu schützen.

3. Ist Internetseite verschlüsselt?

Ob die Verbindung zwischen dem Browser und einer Website verschlüsselt ist, so dass Dritte die ausgetauschten Daten nicht mitlesen können, ist daran ersichtlich, dass die URL (d.h. die Adresse in der Browserzeile) mit «https://…» anstatt nur «http://…» beginnt. Zudem erscheint in allen gängigen Browsern ein Schloss-Icon vor der URL (🔒 | https://).

4. Wie erhalte ich einfachen Zugriff auf die über mich gespeicherten Daten bei Behörde X oder Firma Y?

Die Datenschutzgesetze von Bund und Kantonen statuieren das Recht jeder Person, vom Inhaber einer Datensammlung Auskunft darüber zu erhalten, ob und falls ja welche Daten über sie bearbeitet werden. Auf dieses Recht kann nicht im Voraus verzichtet werden.

5. Transparenz, wer die Daten bekommt und wer nicht?

Sofern der Datenbearbeiter nicht schon bei der Beschaffung der Personendaten angibt, an wen die Daten weitergegeben werden, kann im Rahmen des Auskunftsrechts (siehe Antwort auf Frage 4) Rechenschaft

darüber verlangt werden, welche Kategorien von Daten an welche Kategorien von Datenempfängern weitergegeben werden.

6. Muss der Produzent sein Einverständnis für seine Datenfreigabe periodisch aktualisieren oder reicht einmal?

Eine Einwilligung zur Bearbeitung/Weitergabe von Personendaten ist in jenem Umfang gültig, wie sie erteilt wurde; dies kann unbefristet sein. Allerdings verlangt das Verhältnismässigkeitsprinzip, dass Personendaten nur so lange bearbeitet (inkl. aufbewahrt) werden dürfen, wie es der bei der Beschaffung erkennbare Zweck erfordert – es ist davon auszugehen, dass auch die Einwilligung nur für diese Dauer erteilt wurde. Ist eine bewilligte Datenbearbeitung abgeschlossen, ist für eine spätere «neue» Bearbeitung/Bekanntgabe eine erneute Einwilligung erforderlich (soweit eine solche nötig ist). Eine Einwilligung ist grundsätzlich frei widerrufbar (je nach zugrundeliegendem Vertrag kann ein Widerruf «zur Unzeit» aber eventuell zu Schadenersatzpflicht führen; siehe Antwort auf Frage 17).

7. Wem darf ich welche Daten herausgeben?

Behörden benötigen für eine Bekanntgabe von Personendaten an Dritte eine gesetzliche Grundlage, die ihnen dies erlaubt, oder die Einwilligung der betroffenen Person im Einzelfall. Private Unternehmen dürfen Personendaten nur so bearbeiten (inkl. an Dritte bekanntgeben), wie es bei der Beschaffung für die betroffene Person erkennbar war (z.B. durch eine entsprechende Datenschutzerklärung); eine Weitergabe von besonders schützenswerten Personendaten (z.B. Konfession, politische Ansichten, Gesundheit, Intimsphäre) ist nur bei einem überwiegenden Interesse zulässig.

8. Was ist die Auswirkung des neuen EU-Gesetzes auf die Schweiz?

Die Datenschutz-Grundverordnung der EU (DSGVO) gilt in folgenden Fällen auch für Schweizer Unternehmen: (1) Das Unternehmen hat eine Niederlassung in der EU, die Personendaten bearbeitet oder bearbeiten lässt, oder es lässt Daten durch einen Auftragnehmer in der EU bearbeiten. (2) Das Unternehmen bietet Waren und/oder Dienstleistungen an Personen, die sich in der EU aufhalten, und bearbeitet dabei deren Daten, oder es beobachtet die Internet-Aktivitäten von Personen in der EU (z.B. um auf die Person zugeschnittene Werbung zu präsentieren). Auch Unternehmen in der EU dürfen Personendaten nur in Drittstaaten übermitteln, in denen ein angemessenes Datenschutzrecht gilt (siehe Antwort auf Frage 1). Für die Bekanntgabe von Personendaten in die Schweiz (als Drittstaat) gilt deshalb die DSGVO als Benchmark.

9. Welche rechtlichen Anforderungen muss man berücksichtigen, wenn man z.B. Vorträge aufzeichnet oder Interviews macht? Wie handhabt man den Umgang mit Video-, Ton- und Bildmaterial, das für Schulungen verwendet wird?

Die Personen, die aufgenommen werden sollen, sind vorgängig angemessen über die Aufnahme und deren Zweck (inkl. eine mögliche Verwendung im Rahmen von Schulungen, was einer Bekanntgabe an Dritte entspricht) zu informieren, damit diese freiwillig einwilligen oder eine Aufnahme ablehnen können. Sobald der Zweck einer Aufnahme erfüllt ist, ist diese zu löschen. Bis dahin ist sie gegen unbefugten Zugriff durch Dritte zu schützen.

10. Sind Daten sicher abgelegt?

Wer Personendaten bearbeitet (inkl. aufbewahrt), muss durch angemessene technische und organisatorische Massnahmen sicherstellen, dass die Vertraulichkeit, Verfügbarkeit und Integrität der Daten jederzeit gewährleistet ist. Wie gut ein Datenbearbeiter dieser Pflicht nachkommt, ist in der Praxis schwierig nachprüfbar. Als betroffene Einzelperson (z.B. Kunde) kann man sich vertragliche Zusicherungen machen lassen, deren Einhaltung man aber in der Regel nicht überprüfen kann. Als gewerblicher Datenlieferant kann man sich gegebenenfalls das Recht ausbedingen, die Informationssicherheit vor Ort zu überprüfen. Der EDÖB und die kantonalen Aufsichtsbehörden haben ein weitreichendes Recht auf Auskunft und Einsicht sowie die Möglichkeit, Empfehlungen (auch zur Datensicherheit) auszusprechen und bei Differenzen vor die Verwaltungsgerichte zu bringen.

11. Bedarf an Selbstbestimmung, wer Daten bekommt?

Behörden von Bund und Kantonen dürfen Personendaten nur bearbeiten (inkl. weitergeben), wenn dafür eine genügende gesetzliche Grundlage besteht. Ausnahmsweise kann eine Einwilligung der betroffenen Person eine ungenügende Rechtsgrundlage kompensieren, umgekehrt kann eine Person mit einem schutzwürdigen Interesse verlangen, dass ihre Daten (trotz gesetzlicher Grundlage) nicht weitergegeben werden. Private Datenbearbeiter dürfen Daten (auch ohne Einwilligung der betroffenen Person) an Dritte weitergeben, wenn ihr Interesse an der Weitergabe jenes des/der Betroffenen überwiegt und die Möglichkeit der Weitergabe bei der Beschaffung angegeben wurde oder für die betroffene Person erkennbar war.

12. Wem gehören die Maschinendaten?

Aus Sicht des Datenschutzrechts gibt es kein «Recht» an Daten. Es gibt betroffene Personen, auf die sich die Angaben beziehen, und Datenbearbeiter, die unter bestimmten Voraussetzungen Personendaten bearbeiten (inkl. aufbewahren) dürfen. Auch nur maschinenlesbare Daten sind Personendaten, solange daraus Aussagen über bestimmte oder bestimmbare Personen gewonnen werden können. Dass Datensammlungen (gerade von Personendaten) einen grossen wirtschaftlichen Wert haben können, ist kein vom Datenschutzrecht anerkannter Umstand. Namentlich ist die Realisierung dieses Werts durch eine Weitergabe von Personendaten kein geschütztes Interesse, um die dadurch begangene Persönlichkeitsverletzung zu rechtfertigen.

13. Welche Daten sollen als OGD publiziert werden?

Offene Verwaltungsdaten (Open Government Data, OGD) sind bei der öffentlichen Aufgabenerfüllung erstellte/gesammelte «Daten, die frei, ohne wesentliche rechtliche, finanzielle oder technische Einschränkungen, genutzt, verarbeitet, ausgewertet und weitergegeben werden dürfen. Rechtlich muss die kostenfreie Nutzung und Weiterverarbeitung der Daten gewährleistet sein; technische Offenheit betont, dass offene Daten maschinell bearbeitbar sein müssen. Bei der Publikation von Daten als offenen Daten müssen Datenschutz-, Informationsschutz- und Urheberrechtsbestimmungen sowie Geschäftsgeheimnisse gewahrt bleiben» (OGD-Strategie der Schweiz 2019–2023, Ziffer 3). Eine (im Internet weltweite!) Publikation von Personendaten ist nur mit der Einwilligung der betroffenen Personen zulässig.

14. Was muss bezüglich der DSGVO in der Schweiz berücksichtigt werden?

Siehe Antwort auf Frage 8. Für von der DSGVO betroffene Schweizer Unternehmen hat der EDÖB nützliche Tipps zusammengestellt.

15. Für was verwende ich WhatsApp?

Zwar erfolgt die Übermittlung von Textnachrichten über WhatsApp «End-2-End» verschlüsselt, jedoch setzt die Nutzung von WhatsApp voraus, dass das gesamte Adressbuch des Benutzers mit dem Stammverzeichnis des Betreibers abgeglichen wird. Dabei werden alle Kontakte – auch jene von Personen, die WhatsApp nicht benutzen und deshalb nicht in die Nutzungsbedingungen eingewilligt haben – an den Betreiber (hier sogar mit Sitz im Ausland) übermittelt. Sowohl Behördenmitglieder als auch Private müssten deshalb für eine datenschutzkonforme Nutzung sicherstellen, dass sie in ihrem Adressbuch ausschliesslich Personen führen, die selbst in die Weitergabe ihrer Kontaktdaten eingewilligt haben, was in der Praxis kaum zu bewerkstelligen sein dürfte.

16. Sicherheit der Daten vor Missbrauch (Hacker)?

Siehe Antwort auf Frage 10.

17. Was passiert mit freigegebenen Daten, wenn der Dateninhaber seine Zusage wieder storniert?

Soweit sich eine Datenbearbeitung auf die Einwilligung der betroffenen Person stützt, ist die Bearbeitung zulässig, solange die Einwilligung gilt. Der Widerruf einer gültig erteilten Einwilligung wirkt nicht zeitlich zurück, d.h. bisherige Bearbeitungen bleiben rechtmässig. Für zukünftige Datenbearbeitungen (inkl. das blosse Aufbewahren) fehlt aber der bisherige Rechtsgrund, so dass die Daten unverzüglich gelöscht werden müssen. Erfolgte die Einwilligung im Rahmen eines Vertrags, der den Datenbearbeiter zu mit eigenen

Aufwänden verbundenen Leistungen verpflichtete, so kann ein Widerruf «zur Unzeit» dazu führen, dass dem Vertragspartner der entstandene Schaden (z.B. vergebliche Aufwände) zu ersetzen ist.

18. Comment assurer la protection des données avec tous les échanges qui sont faits (plateformes fédérales, etc.)?

Wer immer Personendaten bearbeitet (inkl. von anderen Bearbeitern entgegennimmt und/oder an andere weiterreicht), ist für die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit verantwortlich. Jeder Beteiligte muss für seinen Bereich sicherstellen, dass (1) eine genügende Rechtsgrundlage bzw. ein Rechtfertigungsgrund besteht und (2) die Grundsätze der rechtskonformen Datenbearbeitung (insbesondere Zweckbindung und Verhältnismässigkeit) eingehalten werden. Die Eigenverantwortung der Datenbearbeiter wird «verstärkt» durch die Aufsicht von Aufsichtsbehörden, die von sich aus oder auf Meldung Dritter die Einhaltung des Datenschutzrechts überprüfen können, sowie die Rechte der betroffenen Personen auf Auskunft/Einsicht in die über sie bearbeiteten Daten und auf Berichtigung oder Löschung unzutreffender bzw. nicht mehr benötigter Daten.

19. Qui est véritablement propriétaire des données enregistrées sur les différentes plateformes ou dans les différents programmes?

Siehe Antwort auf Frage 12.

20. Comment assurer la sécurité des données sans entraver la fluidité du travail?

Das Datenschutzrecht ist ein risikobasiertes Recht. Deshalb müssen die technischen und organisatorischen Massnahmen zum Schutz von Personendaten *angemessen* sein. Was als angemessen gilt, richtet sich namentlich nach dem Zweck, der Art und dem Umfang der Datenbearbeitung, den möglichen Risiken für die betroffenen Personen sowie dem aktuellen Stand der Technik. Mittels geeigneter Massnahmen ist zu erreichen, dass die Restrisiken (beurteilt nach Eintretenswahrscheinlichkeit und Schaden im Fall des Eintretens) auf ein tragbares Mass reduziert werden. Eine hundertprozentige Sicherheit gibt es nie.