In der Krise ist nicht alles anders

Auch in der Krise nicht alles offenlegen

Gerade in der Krise sind Einwohnerinnen und Einwohner auf den Schutz ihrer Grundrechte angewiesen. Grundrechte wie der Datenschutz dürfen nur eingeschränkt werden, wenn eine rechtliche Grundlage dies erlaubt und die Einschränkung geeignet und erforderlich ist, einen angestrebten Zweck zu erreichen.

Ein Vater wandte sich kurz vor den Sommerferien an die Datenschutzbeauftragte. Die Primarschule seines Kindes verlangte in einem Elternbrief die Offenlegung aller Reisepläne der Eltern und der Kinder in Länder, für die zum damaligen Zeitpunkt Quarantänebestimmungen galten.

Abklärungen der Datenschutzbeauftragten ergaben, dass die Schule eine Vorlage mit Textbausteinen des Volksschulamtes (VSA) missverstanden hatte. Die Offenlegung von Reiseplänen vor den Sommerferien ist weder erforderlich noch geeignet, um Ansteckungen mit dem Coronavirus zu verhindern. Die Eltern sind somit nicht dazu verpflichtet.

Auf Nachfrage der Datenschutzbeauftragten bestätigte das VSA, dass lediglich nach den Ferien eine Informationspflicht der Eltern gelte, wenn ein Kind infolge Quarantäne den Unterricht nicht besuchen kann. Die Vorlage des VSA enthielt keinen Hinweis auf eine Pflicht zur Information über Reisepläne. Das VSA hatte mit dem Elternbrief vor den Sommerferien beabsichtigt, die Eltern und Schülerinnen und Schüler an die Quarantänebestimmungen zu erinnern und den Hinweis anzubringen, dass kein Anspruch auf Fernunterricht bestehe.

Die Datenschutzbeauftragte half der Schule noch vor den Sommerferien, die Probleme mit dem Elternbrief zu bereinigen, und riet, die Eltern sofort aufzuklären. Sie wies die Schule auf die Pflicht hin, bisher erhaltene Daten über Ferienpläne und Destinationen zu löschen.

Einheitliche Regelung statt Chaos

Die Quarantäneregelungen hatten Konsequenzen für den Schulbetrieb nach den Ferien. Die Datenschutzbeauftragte informierte, dass das aktive Abfragen von Reisedestinationen auch nach den Ferien nicht Aufgabe der Schule und Lehrpersonen sei. Die Schulen bekamen von verschiedenen Seiten andere Ratschläge. Sie stellten sich die Frage, wie sie nach den Schulferien mit der Situation umgehen sollten. Die Schulen haben eine Fürsorgepflicht und müssen gewisse Massnahmen zur Prävention übertragbarer Krankheiten treffen. Das VSA wollte mit einem Leitungszirkular für Klarheit sorgen.

Das VSA erinnerte im Leitungszirkular daran, dass die Eltern für die Einhaltung der Quarantäne selbst verantwortlich sind und darüber bereits vor den Sommerferien informiert worden waren. Es hielt nochmals fest, dass die Schulen keine eigenen Nachforschungen zur Abklärung oder Überprüfung der Quarantänepflicht tätigen. Die Schule oder das Lehrpersonal sollten jedoch die betroffenen Eltern nochmals über ihre Verantwortlichkeit informieren, wenn sie vermuteten, dass sich eine Schülerin oder ein Schüler in Quarantäne befinden sollte. Wussten sie von der Quarantänepflicht einer Schülerin oder eines Schülers, sollte sie

respektive er nach Hause geschickt sowie die Eltern und der kantonale Schulärztliche Dienst informiert werden. Der Schulärztliche Dienst würde das weitere Vorgehen mit dem Kantonsärztlichen Dienst koordinieren. Die Quarantäne sollte wie Abwesenheit wegen Krankheit behandelt werden.

Die Datenschutzbeauftragte beurteilte die Regelungen des VSA als datenschutzkonform.

Fragen zum Gesundheitszustand vor Prüfungen

Eine Hochschule kontaktierte die Datenschutzbeauftragte in ihren Vorbereitungen auf die Prüfungen, die nach dem Lockdown wieder vor Ort stattfinden sollten. Den Prüfungskandidatinnen und -kandidaten sollte schriftlich mitgeteilt werden, dass sie nur an den Prüfungen teilnehmen dürfen, wenn sie sich absolut gesund fühlen. Zusätzlich erarbeitete die Schule einen Fragebogen zum Gesundheitszustand der Kandidatinnen und Kandidaten.

Personendaten dürfen bearbeitet werden, wenn dies zur Erfüllung der gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist. Die Bearbeitung besonderer Personendaten wie Gesundheitsdaten muss in einem formellen Gesetz geregelt sein.

Die Datenschutzbeauftragte hielt fest, dass für den Fragebogen zum Gesundheitszustand verschiedene Bestimmungen als rechtliche Grundlage herbeigezogen werden können. Der Einsatz des Fragebogens muss jedoch auch durch ein öffentliches Interesse gerechtfertigt und verhältnismässig sein.

Die Hochschule wollte mit dem Fragebogen Personen davon abhalten, trotz Krankheit oder Symptomen an den Prüfungen zu erscheinen. Die Datenschutzbeauftragte befand, dass das Abfragen von Krankheitserscheinungen oder Unwohlbefinden für diesen Zweck nicht geeignet sei. Die Befragten könnten den Fragebogen trotz Krankheit mit «gesund» oder «keine Symptome» ausfüllen. Die Datenschutzbeauftragte schlug vor, die Punkte des Fragebogens als Hinweis in die vorbereitete Covid-Richtlinie für Prüfungen aufzunehmen. Alle Prüfungskandidatinnen und -kandidaten seien darüber aufzuklären, dass sie bei Vorliegen von Symptomen nicht an einer Prüfung erscheinen dürfen. Zu Dokumentationszwecken und um die Hürde für die Umgehung zu erhöhen, könnte verlangt werden, die Kenntnisnahme der Regeln mit der Unterschrift zu bestätigen. Dadurch wird dieselbe Wirkung erzielt wie durch den Fragebogen, ohne dass Gesundheitsdaten gespeichert werden.

Fluggastdaten zur Kontrolle der Meldepflicht

In der Sommerferienzeit waren die Fluggesellschaften verpflichtet, die Kontaktdaten von Flugpassagieren aufzunehmen und dem Bundesamt für Gesundheit (BAG) abzuliefern. Das BAG sollte die Daten danach an die Kantone übermitteln, damit diese die Meldepflicht für Reisende aus Risikoländern kontrollieren konnten. Der Kanton Zürich sah in diesem Vorgehen eine Gefahr von zeitlichen Verzögerungen. Er setzte die Kantonspolizei ein, um die Kontaktdaten direkt bei den Fluggesellschaften abzuholen und der Gesundheitsdirektion auszuhändigen.

Die Datenschutzbeauftragte erfuhr von diesem Vorgehen zunächst aus den Medien. Nachträglich entstand ein konstruktiver Austausch mit der Sicherheitsdirektion. Sie konsultierte die Datenschutzbeauftragte zu den Bemühungen des Kantons, das bereits praktizierte Vorgehen mit dem BAG schriftlich zu regeln. Der Kanton Zürich übernahm die digitale Erfassung der Kontaktkarten der Fluggesellschaften auch für andere Kantone. Die Datenschutzbeauftragte erhielt die Gelegenheit, das Vorgehen bei der Erfassung der Kontaktdaten vor Ort zu überprüfen. Gestützt auf ihre Beobachtungen regte sie Anpassungen der Bearbeitungsprozesse an.

Datenschutz im Datenüberfluss

Die Gesundheitsdirektion musste beim Contact Tracing grosse Mengen Personendaten bearbeiten. Dabei handelte es sich um Gesundheitsdaten und somit besondere Personendaten. Dies verlangte besondere Aufmerksamkeit beim Datenschutz. Die betroffenen Personen mussten sich auch in Krisenzeiten auf den Schutz ihrer Privatsphäre verlassen können. Die Gesundheitsdirektion arbeitete eng mit der Datenschutzbeauftragten zusammen.

Kontrolle über Contact-Tracing-Daten behalten
Mitte Juli 2020 wurde die Gesundheitsdirektion beauftragt, die Kapazitäten des Contact Tracings auszubauen, um die Nachverfolgung von mindestens 100 Neuinfektionen pro Tag gewährleisten zu können. Sie vergab einen Teil des Contact Tracings an eine private Firma, um den Kantonsärztlichen Dienst zu entlasten. Die Gesundheitsdirektion wandte sich an die Datenschutzbeauftragte, um die Einhaltung der datenschutzrechtlichen Vorgaben bei diesem Outsourcing zu überprüfen. Die Datenschutzbeauftragte gab rasch konkrete Anregungen zur Erstellung eines Informationssicherheitskonzeptes sowie zu den datenschutzrechtlichen Bestimmungen. Somit konnte sichergestellt werden, dass die Gesundheitsdirektion die Verantwortung und die Kontrolle über die Contact-Tracing-Daten und ihre Sicherheit behält.

Sicherer Umgang mit Daten quarantänepflichtiger Personen
Aufgrund von Vorschriften des Bundes müssen sich Personen bei der Einreise aus einem Risikoland bei der Gesundheitsdirektion melden und in Quarantäne gehen. Die Gesundheitsdirektion wollte diese Meldepflicht für die Einreisenden so einfach wie möglich gestalten. Dafür musste sie im Sommer 2020 innert weniger Tagen ein mehrsprachiges Online-Formular bereitstellen. Die Datenschutzbeauftragte beriet die Gesundheitsdirektion, wie sie die Informationssicherheit bei der Bearbeitung der Daten von quarantänepflichtigen Personen einhalten kann, beispielsweise durch die Verwendung verschlüsselter E-Mails und Excel-Dokumente sowie dem Einsatz von sicheren Webtransfers.

Covid-19-Schutzkonzepte und der Schutz der Personendaten
Eine Kantonsratsanfrage befasste sich mit dem Schutz von Personendaten im Rahmen von Covid-19-Schutzkonzepten. Für die Antwort lud die Gesundheitsdirektion die Datenschutzbeauftragte zum Mitbericht ein. Die Datenschutzbeauftragte wies darauf hin, dass die Datenbearbeitung durch private Betriebe wie Restaurants unter die Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) fallen. Die Datenschutzbeauftragte ist für die Aufsicht über die Datenbearbeitungen der öffentlichen Organe im Kanton Zürich zuständig. Bei Anfragen im Zusammenhang mit der datenschutzrechtlichen Umsetzung der Schutzkonzepte durch öffentliche Organe hat sie diese beraten.

Bedenken bei Angabe von Kundenkontakten
Die Datenschutzbeauftragte erhielt eine Anfrage einer gemeinnützigen Institution, die junge Erwachsene zur Berufsintegration berät. Die jungen Erwachsenen werden von der IV und vom RAV vermittelt. Die Institution wollte wissen, wie sie mit der Aufforderung zur Weitergabe der Kontaktangaben umgehen solle. Die Personendaten geben Auskunft über die aktuelle soziale oder gesundheitliche Situation der Personen. Sie sind deshalb als sensitiv einzustufen. Die Datenschutzbeauftragte erklärte, dass die Bekanntgabe der

Personendaten an den Kantonsärztlichen Dienst durch das Epidemiengesetz gerechtfertigt sei. Sie riet der Institution, die jungen Erwachsenen darauf aufmerksam zu machen, dass sie ihre Daten dem Kantonsärztlichen Dienst auf Aufforderung bekanntgeben muss.

Corona-Infizierte haben ein Recht auf Datenschutz

Beim Contact Tracing werden Personen angerufen und mit der Information konfrontiert, dass einer ihrer Kontakte mit Corona infiziert ist. Das weckt Ängste und führt zu einschneidenden Einschränkungen durch die Quarantänepflicht. Häufig wird den Contact Tracern die Frage gestellt, wer die Kontaktperson mit dem positiven Testresultat sei. Die Gesundheitsdirektion bat die Datenschutzbeauftragte um eine Stellungnahme, ob die Identität der infizierten Person – Indexfall genannt – bekanntgegeben werden dürfe.

Diese Information ist wichtig für Personen, die sich gegen eine Quarantäneanordnung zur Wehr setzen möchten. Sie erhalten eine begründete Verfügung, gegen die sie auf dem Rechtsweg vorgehen können. Es ist kaum möglich, eine Begründung zu formulieren, ohne die Identität des Indexfalls bekanntzugeben. Für die erkrankte Person ist es jedoch ein zusätzlicher einschneidender Eingriff in ihre Persönlichkeitsrechte, wenn ihre Infektion allen Kontaktpersonen bekanntgegeben wird. Bei einem Infektionsfall in einem Restaurant würde so möglicherweise eine sehr persönliche Information einer erheblichen Zahl von Personen bekanntgegeben.

Die Datenschutzbeauftragte betonte, dass die Bekanntgabe der Identität der infizierten Person nur zulässig ist, wenn sie für den Zweck des Contact Tracings notwendig ist. Nach Gesprächen mit der Gesundheitsdirektion regte sie ein schrittweises Vorgehen an. Zunächst ist der Indexperson vorzuschlagen, Kontaktpersonen selbst zu informieren. Als weitere Möglichkeit kann sie gefragt werden, ob sie der Bekanntgabe ihrer Identität zustimme. Wenn die Indexperson beides ablehnt, ist eine Quarantäneanordnung ohne Personenbezug zu begründen. Die infizierte Person ist nur eindeutig zu identifizieren, wenn die Begründungspflicht dies verlangt, etwa wenn eine Kontaktperson den Rechtsweg beschreiten möchte.

Keine Weitergabe von Contact-Tracing-Daten für Strafuntersuchung

Ein Restaurantbesitzer fragte die Datenschutzbeauftragte an, ob er verpflichtet ist, Kontaktdaten seiner Gäste an die Kantonspolizei herauszugeben. Die Ermittlung betraf ein schwerwiegendes Gewaltdelikt in unmittelbarer Nähe seines Restaurants.

Die Kontaktdaten sind zweckgebunden für das Contact Tracing erhoben worden. Bei einer Strafuntersuchung können auch Informationen genutzt werden, die in einem anderen Zusammenhang gesammelt wurden. Dafür gelten allerdings Einschränkungen. Eine umfassende Beweisausforschung ist nicht erlaubt. Gezielte Ermittlungen bei einem konkreten Tatverdacht sind erlaubt. Der Restaurantbesitzer muss also nur die Kontaktdaten mit einem nahen Bezug zur Straftat herausgeben, beispielsweise der männlichen Gäste, die zu einem bestimmten Zeitpunkt das Restaurant verliessen, falls diese Kriterien für die Ermittlungen relevant sind.

Anonyme Auswertung von Contact-Tracing-Daten

In den Anfangszeiten der Pandemie mangelte es an epidemiologischen Daten. Die Zusammenarbeit zwischen der Gesundheitsdirektion und dem Statistischem Amt sollte diese Situation verbessern. Dafür wurden grosse Mengen von Personendaten mit Gesundheitsbezug bearbeitet. Auf Anregung der Gesundheitsdirektion unterstützte die Datenschutzbeauftragte die Beteiligten bei der Ausarbeitung einer Zusammenarbeitsvereinbarung. Sie stellte dabei sicher, dass die Verantwortlichkeit für die Privatsphäre der betroffenen Personen angemessen geregelt wurde.

Mit Doodle zum Gottesdienst anmelden

Nach dem Lockdown im Frühling 2020 wurde auch ein Schutzkonzept für den Kirchenbesuch entwickelt. So war die Anzahl der teilnehmenden Personen begrenzt und ihre Kontaktdaten mussten registriert werden. Eine Kirchgemeinde wollte die Registrierung über das Online-Terminplanungstool Doodle lösen. Ein Journalist wandte sich an die Datenschutzbeauftragte und wies darauf hin, dass die Kontaktdaten öffentlich einsehbar waren.

Angaben zu religiösen Aktivitäten sind besondere Personendaten. Die Datenschutzbeauftragte erklärte, dass eine telefonische Anmeldung den Schutz der Privatsphäre am besten gewährleisten würde. Wenn die personellen Ressourcen dafür in der aktuellen Krise fehlten, könnten auch Kirchgemeinden auf digitale Kanäle ausweichen. Bei der Wahl des Produkts sind die wichtigsten Anforderungen zu berücksichtigen, vor allem der Speicherort der Daten. Werbefinanzierte Gratisangebote sind für solche Zwecke ungeeignet.

Bei der Nutzung des Produkts steht die Privatsphäre der Kirchgängerinnen und Kirchgänger im Vordergrund. Eingebaute Schutzmassnahmen wie die anonymisierte Darstellung erhöhen die Vertraulichkeit. Allerdings kann die Kirche deren Zuverlässigkeit nicht vollständig abklären.

Deshalb sind weitere Massnahmen zu treffen. Besonders geeignet ist die Verwendung von Pseudonymen oder Initialen. Eine geschickte Kombination von Vorsichtsmassnahmen kann zu einer Lösung führen, die in der aktuellen besonderen Situation vertretbar ist.

Gemeinde-versammlung im Fernsehen

Gemeindeversammlungen sind im Kanton Zürich öffentlich. Jede Person kann als Gast teilnehmen, ohne ein besonderes Interesse anmelden zu müssen. Das Prinzip der Öffentlichkeit kennt jedoch Einschränkungen.

Dies illustriert der Fall eines Bürgers, der sich in einer Nachrichtensendung bei der Abstimmung an der Gemeindeversammlung wiedererkannte. Die Datenschutzbeauftragte hielt fest, dass Bild- und Tonaufnahmen an Gemeindeversammlungen nur erlaubt sind, wenn sie die Stimmberechtigten nicht beeinträchtigen.

Zulässig sind Gesamtaufnahmen, bei denen die einzelnen Stimmberechtigten nicht erkennbar sind. Die Versammlungsleitung hat die Teilnehmenden über die Aufnahmen zu informieren. Aufnahmen während Wahlen und Abstimmungen sind nicht zulässig. Der Schutz des Wahlgeheimnisses und der freien Meinungsbildung ist unter diesen Voraussetzungen gewährleistet.

Universalschlüssel zu den Bibliotheken

Die neue nationale Lösung Swisscovery soll den Zugang zu allen Bibliotheken der Schweiz ermöglichen. Jede Person kann mit einem einzigen Konto entsprechend ihrer Berechtigungen Bücher ausleihen. Swisscovery wird durch die Swiss Library Services Platform (SLSP) betrieben.

Die Universitäten Bern, Basel und Zürich meldeten Swisscovery bei den kantonalen Datenschutzbehörden zur Vorabkontrolle an. Die zuständigen Datenschutzbehörden dieser Kantone arbeiteten bei der Vorabkontrolle aufgrund der schweizweiten Bedeutung des Projekts zusammen. Bei kantonsübergreifenden Projekten fand schon früher ein Austausch zwischen verschiedenen Aufsichtsbehörden statt. Das vollständig koordinierte Vorgehen beim Swisscovery-Projekt war neu.

Die zentrale Herausforderung von Swisscovery lag in der Vielfalt der angeschlossenen Institutionen. Swisscovery muss sehr unterschiedlichen Bedürfnissen entgegenkommen, von grossen Institutionen wie der Universität Zürich und kleinen wie beispielsweise der Jesuitenbibliothek sowie Nutzenden unterschiedlicher Altersgruppen. Gleichzeitig müssen Institutionen aus dem privatwirtschaftlichen Bereich und aus allen Kantonen berücksichtigt werden. Die Datenschutzbehörden setzten sich in der Vorabkontrolle mit den vielen verschiedenen Rechtsgrundlagen auseinander, die zur Anwendung kommen. Die kantonalen Gesetze sehen die Teilnahme an Plattformen teilweise nicht ausdrücklich vor. Deshalb regten die Datenschutzbehörden für den Kanton Zürich an, eine konkrete Rechtsgrundlage zu schaffen. Weiter prüften sie die vertraglichen Grundlagen zwischen Institutionen und der SLSP und die technische Umsetzung der Plattform. Swisscovery kann ausschliesslich mit einer edu-ID genutzt werden. Die edu-ID wird durch die Stiftung Switch herausgegeben und wurde zur Identifizierung im schweizerischen Bildungssystem entwickelt. Die Datenschutzbehörden hinterfragten diese Anbindung kritisch. Sie regten Verbesserungen beim Registrierungsprozess der Nutzerinnen und Nutzer an. Sie sind transparent zu informieren, welcher Anbieter welche Personendaten bearbeitet.

Die Vorabkontrolle konnte nach mehreren Nachlieferungen der Institutionen abgeschlossen werden. Die Datenschutzbeauftragten halten im Bericht fest, dass der datenschutzkonforme Betrieb der Plattform möglich ist. Allerdings sind Nachbesserungen nötig. Dabei geht es einerseits um einzelne Aspekte, wie dem Umgang mit Cookies und der Optimierung interner Prozesse. Andererseits stellte sich die Grundsatzfrage nach einer wirksamen Kontrolle der Plattform. Die teilnehmenden Bibliotheken müssen die Möglichkeit haben, Audits durchzuführen oder zu veranlassen. Die Erfahrung der Datenschutzbeauftragten zeigt, dass die Überwachung der Anbieter schwierig zu koordinieren ist, wenn bei Projekten zahlreiche Institutionen in verschiedenen Kantonen beteiligt sind. Im Vorabkontrollbericht werden die Universitäten Bern, Basel und Zürich aufgefordert, Koordinationsmöglichkeiten zu prüfen.

Zudem beriet die Datenschutzbeauftragte einzelne Institutionen zu konkreten Umsetzungsfragen. Im Vordergrund stand der Zugang zu den Bibliotheken für Nutzerinnen und Nutzer ohne eigene E-Mail-Adresse.

Die Datenschutzbeauftragte wird die Entwicklungen bei Swisscovery weiter verfolgen und überwachen.

Rayonverbot mit Electronic Monitoring

Electronic Monitoring (EM), auch als elektronische Fussfessel bekannt, wird im Straf- und Massnahmenvollzug sowie als strafprozessuale Ersatzmassnahme eingesetzt. Künftig wird EM auch im Zivilrecht als präventive Massnahme zum Schutz gewaltbetroffener Personen angewandt, also zur Überwachung eines Rayonverbots.

EM ist die räumliche und zeitliche Überwachung einer Person. Die betroffene Person trägt einen elektronischen Sender. Der Sender übermittelt die Standortdaten an den EM-Server. Zur Ortung der überwachten Person wird entweder die Radiofrequenz-Technologie oder das Global Positioning Service (GPS) verwendet. Die Datenübertragung vom Sender zu den Servern erfolgt über das Mobiltelefonnetz.

Bei der räumlichen und zeitlichen Überwachung von Personen wird eine grosse Menge an sensitiven Personendaten bearbeitet. Da sie beim EM in Zusammenhang mit einer administrativen oder strafrechtlichen Verfolgung oder Sanktion bearbeitet werden, handelt es sich zudem um besondere Personendaten. Ihre Erfassung und weitere Bearbeitung stellen besondere Anforderungen an den Datenschutz und die Informationssicherheit. Die Datenschutzbeauftragte begrüsst es, dass ihre Behörde in den vergangenen Jahren mehrmals in das Projekt einbezogen wurde. Im Jahr 2013 prüfte sie die Ausschreibungsunterlagen für die EM-Technik und die Überwachungszentrale. Bei der Überführung vom Pilot- in den Regelbetrieb im Jahr 2018 prüfte sie die Massnahmen zum Datenschutz und zur Informationssicherheit.

2020 stellte sie fest, dass die Anforderungen an Datenschutz und Informationssicherheit als zentrale Punkte beim Betrieb des EM bereits weitgehend berücksichtigt und umgesetzt wurden. Als problematisch erachtete sie, dass das System auch Überwachungsdaten erfasst und Meldungen absetzt, wenn dies zur Überwachung der Auflagen nicht erforderlich ist. Die Ortung findet auch statt, wenn die Person die Auflagen nicht verletzt. Sie verlangte, dass diese widerrechtlich bearbeiteten Informationen zeitnah gelöscht werden.

Am Betrieb des EM sind neben öffentlichen Organen auch private Unternehmen beteiligt. Wenn Private im Auftrag eines öffentlichen Organs handeln, gelten für sie in Bezug auf Geheimhaltung und Informationssicherheit die gleichen Pflichten. Die Datenschutzbeauftragte konnte die Verträge der beauftragten Privaten nicht prüfen. Sie wies aber darauf hin, dass die kantonalen Vorgaben zur Informationssicherheit auf die Privaten zu übertragen sind. In Zusammenarbeit mit dem öffentlichen Organ konnten zahlreiche weitere Aspekte geklärt werden.

In Zukunft wollen alle Kantone der Schweiz die gleiche EM-Technologie und eine gemeinsame Überwachungszentrale betreiben. Die Datenschutzbeauftragte beteiligt sich in einer Arbeitsgruppe der Konferenz der schweizerischen Datenschutzbeauftragten privatim zu diesem Thema. Sie unterstützt die Projektleitung in Datenschutzfragen.