

Wirksame neue Instrumente

- 42 Datenschutz-Folgenabschätzung wird Pflicht
- 43 Datenschutzvorfälle müssen gemeldet werden



Datenschutz-Folgenabschätzung wird Pflicht

Seit Juni 2020 sind öffentliche Organe verpflichtet, eine Datenschutz-Folgenabschätzung (DSFA) zu erstellen. Bei neuen Datenbearbeitungen sollen im Voraus die Risiken für die Privatsphäre eingeschätzt und minimiert werden. Die Datenschutzbeauftragte hatte öffentliche Organe schon immer im Umgang mit Privatsphärischen Risiken unterstützt. Neu ist die ausdrückliche gesetzliche Pflicht, ein entsprechendes Dokument zu erstellen.

Die Datenschutzbeauftragte erstellte ein Formular und ein Merkblatt, das die datenbearbeitenden Stellen bei der Datenschutz-Folgenabschätzung unterstützt. Es hilft, alle wesentlichen Angaben zu sammeln und auszuwerten. Erste Erfahrungen zeigen, dass das Formular und das Merkblatt zweckmässig sind. Die Datenschutzbeauftragte erhielt von mehreren Organen vollständige und aussagekräftige Analysen.

Die DSFA dient auch dazu, die Pflicht zur Vorabkontrolle abzuklären. Wenn besondere Risiken erkennbar sind, muss das Projekt der Datenschutzbeauftragten zur Vorabkontrolle unterbreitet werden. Die DSFA macht die Beurteilung der Vorabkontrollpflicht sowohl für die Organe als auch für die Datenschutzbeauftragte transparenter. In Projekten ohne Vorabkontrollpflicht ist die DSFA ein internes Arbeitsinstrument. Die Datenschutzbeauftragte steht auch in solchen Fällen für einen Austausch zur Verfügung.

Die DSFA ist neu Teil der Projektmanagement-Methode Hermes. Die Datenschutzbeauftragte konnte in Zusammenarbeit mit dem Competence Center für Projektmanagement (CCPM) klären, in welcher Projektphase eine DSFA zu erstellen ist. Damit ist sichergestellt, dass bei Projekten in der kantonalen Verwaltung die Datenschutzrisiken rechtzeitig und korrekt adressiert werden.

Projektverantwortliche nehmen den Datenschutz manchmal nur als zusätzliche Hürden wahr, oft sogar als Hindernis. Die Datenschutzbeauftragte sieht es als ihre Aufgabe, Projektverantwortliche davon zu überzeugen, dass Datenschutz das Resultat ihrer Arbeit verbessern kann. Dafür müssen die Anforderungen des Datenschutzes rechtzeitig in die Projektentwicklung integriert werden. Die DSFA mag auf den ersten Blick als lästige Pflicht erscheinen. Auf den zweiten Blick bietet sie eine Chance, einen Mehrwert für ein Projekt zu schaffen.

Das Formular und das Merkblatt zur Datenschutz-Folgenabschätzung sind auf der Website der Datenschutzbeauftragten www.datenschutz.ch unter Datenschutz in öffentlichen Organen publiziert.

Datenschutz- vorfälle müssen gemeldet werden

Im Juni 2020 trat das revidierte Gesetz über die Information und den Datenschutz (IDG) in Kraft. Seitdem sind öffentliche Organe verpflichtet, Datenschutzvorfälle an die Datenschutzbeauftragte zu melden. Meldepflichtig ist beispielsweise, wenn sich eine Hackerin oder ein Hacker Zugriff auf Daten verschafft oder auch wenn ein Mitarbeiter oder eine Mitarbeiterin einen USB-Stick mit Personendaten verloren hat.

Die Datenschutzbeauftragte erstellte ein Formular, um Datenbearbeitenden die Meldung zu erleichtern. Dafür arbeitete sie zusammen mit Datenschutzaufsichtsbehörden anderer Kantone, in denen die Meldepflicht eingeführt wurde. Ebenfalls verfügbar ist ein Merkblatt, das die wichtigsten Fragen beantwortet, etwa welche Vorfälle meldepflichtig sind und wie bei der Meldung vorzugehen ist.

Die Bandbreite möglicher Reaktionen der Datenschutzbeauftragten reichen von blosser Kenntnisnahme bis zur umfangreichen Kontrolle vor Ort. Deshalb definierte die Datenschutzbeauftragte einen Bearbeitungsprozess. In einem ersten Schritt klärt sie den Sachverhalt mit der meldenden Stelle. Wenn ein Vorfall meldepflichtig ist, untersucht die Datenschutzbeauftragte ihn und definiert Massnahmen. Sie können einerseits zur Bewältigung des Geschehenen dienen. Andererseits sind Massnahmen zu treffen, um ähnliche Vorfälle in der Zukunft zu vermeiden. Das öffentliche Organ erhält die Massnahmen mit einer Umsetzungsfrist mitgeteilt. Die Datenschutzbeauftragte stellt mit dem internen Prozess eine wirksame Unterstützung des meldenden Organs sicher.

Kurz nach Inkrafttreten des revidierten IDG gingen die ersten Meldungen ein. Auch vor Inkrafttreten war die Datenschutzbeauftragte vereinzelt auf Missstände hingewiesen worden. Die Einführung der Pflicht liess die Anzahl der Meldungen schnell stark ansteigen. Es ist damit zu rechnen, dass sich dieser Trend fortsetzt. Das Wissen um die Meldepflicht muss sich bei den öffentlichen Organen weiterverbreiten. Dafür sorgt die Datenschutzbeauftragte auch in ihren Weiterbildungsaktivitäten.

Die Datenschutzbeauftragte behandelt die Vorfälle vertraulich und setzt bei der Bewältigung bewusst auf ein kooperatives Vorgehen. Die meldepflichtigen Organe schätzen die konstruktiven Anregungen.

Die Datenschutzbeauftragte musste auch entscheiden, wie sie mit meldepflichtigen Vorfällen umgeht, die sie aus anderen Quellen erfährt. In den Medien wurde beispielsweise über einen Cyberangriff in ihrem Zuständigkeitsbereich berichtet. In diesen Fällen nimmt die Datenschutzbeauftragte Kontakt mit dem betroffenen Organ auf und klärt, ob der Vorfall meldepflichtig ist.

Die bisher gemeldeten Vorfälle sind vielfältig. Eine Behörde sendete Belege an die falsche Person. Ein Spital sendete Patienteninforma-



tionen an die falsche Adressatin. Eine Behörde entsorgte Rechner ohne ausreichende Datenlöschung. Ein vor Jahren entwendetes Dokument wurde dem Absender von einem Unbekannten zugespielt.

Nach der Bearbeitung der ersten Meldungen ist klar, dass die Information der Betroffenen meist die zentrale Frage darstellt. Die Datenschutzbeauftragte kann von der meldenden Stelle verlangen, dass die Betroffenen über den Vorfall informiert werden. In welchen Fällen dies notwendig ist, will die Datenschutzbeauftragte mit einem standardisierten Entscheidungsprozess beurteilen.

Die ersten Erfahrungen zeigen, dass die gemeinsame Bearbeitung der Vorfälle durch die Datenschutzbeauftragte und das öffentliche Organ zu deutlichen Verbesserungen beim Schutz der Privatsphäre führen kann. Die konkrete Behandlung von Datenschutzvorfällen entwickelt präventive Wirkung.

Die gemeldeten Datenschutzvorfälle eignen sich als Anschauungsbeispiele in Weiterbildungen der Datenschutzbeauftragten. Nichts bleibt so gut im Gedächtnis haften wie die Praxisbeispiele dazu, was in der Vergangenheit schiefgegangen ist und wie die Lösung aussieht.

Das Formular und das Merkblatt für die Meldepflicht von Datenschutzvorfällen sind auf der Website der Datenschutzbeauftragten www.datenschutz.ch unter Datenschutz in öffentlichen Organen publiziert.

Verwaltungsmassnahmen zum Einsatz bereit

Das revidierte IDG ermöglicht der Datenschutzbeauftragten, Verwaltungsmassnahmen zu ergreifen. Wenn sich ein Organ nicht an eine Empfehlung der Datenschutzbeauftragten hält, kann sie eine Verfügung aussprechen. Sie kann beispielsweise den Abbruch einer Datenbearbeitung oder die Löschung von Daten verfügen. Diese Möglichkeit kam noch nicht zur Anwendung. Der konstruktive und kooperative Umgang zwischen der Datenschutzbeauftragten und den beaufsichtigten Organen hat sich bewährt. Die Datenschutzbeauftragte ist jedoch vorbereitet. Das neue und schärfste Aufsichtsinstrument steht zum Einsatz bereit.