dsb
datenschutzbeauftragter
kanton zürich

Ziele, Umfang, Ablauf Datenschutzreview

Inhalt

1 Ziele des Datenschutzreviews 2
2 Gesetzliche Grundlagen 2
3 Umfang und Inhalt der Kontrolle 2
3.1 Recht 2
3.2 Organisation und Technik 3
4 Ablauf 4
4.1 Vor Beginn der Kontrolle einzureichende Unterlagen 4
4.2 Prüfung der eingereichten Unterlagen 5
4.3 Vorbesprechung der Kontrolle vor Ort 6
4.4 Überprüfung mit System-, Netz- und Webscanner 6
4.5 Kontrolle vor Ort 6
4.6 Schlussbesprechung 6
4.7 Bericht 6
4.8 Umsetzung der Massnahmen 6

1 Ziele des Datenschutzreviews

Im Rahmen des Datenschutzreviews kontrolliert der Datenschutzbeauftragte (DSB) die Umsetzung der rechtlichen, organisatorischen und technischen Aspekte mittels der eingereichten Unterlagen und der vor Ort vorgefundenen Massnahmen.
Zusätzlich bewirkt die Kontrolle eine Sensibilisierung in Bezug auf einen wirksamen Datenschutz und eine angemessene Sicherheit der Informationstechnologie (IT).

2 Gesetzliche Grundlagen

Der DSB überwacht die Anwendung der Vorschriften über den Datenschutz (§ 34 lit. c Gesetz über die Information und den Datenschutz (IDG)). Er kann ungeachtet allfälliger Geheimhaltungspflichten bei öffentlichen Organen oder beauftragten Dritten schriftlich oder mündlich Auskünfte über das Bearbeiten von Personendaten einholen, Einsicht in Unterlagen und Akten nehmen und sich Bearbeitungen vorführen lassen, soweit es für seine Tätigkeit notwendig ist (§ 35 Abs. 1 IDG). Gemäss § 35 Abs. 2 IDG sind die verantwortlichen Organe verpflichtet, an der Feststellung des Sachverhalts mitzuwirken.

Diese umfassenden Auskunfts- und Einsichtsbefugnisse des DSB werden durch eine entsprechende Schweigepflicht abgesichert. So sind der DSB und seine Mitarbeitenden hinsichtlich Personendaten, die sie bei ihrer Tätigkeit zur Kenntnis nehmen, zur gleichen Verschwiegenheit verpflichtet wie das bearbeitende Organ (§ 38 IDG).

3 Umfang und Inhalt der Kontrolle

3.1 Recht

Es wird geprüft,

- ob die kontrollierte Stelle die rechtlichen Grundlagen für den Zugriff einer anderen Verwaltungsstelle auf besondere Personendaten vorweisen kann und ob diese Grundlagen ausreichen (insbesondere auch für regelmässige Meldungen),
- ob und wie bei Auftragnehmenden, die bei ihrer Leistungserbringung potenziell Zugang zu Personendaten haben, der Datenschutz durch die Verträge gewährleistet wird,
- ob für Personendaten die Aufbewahrungsfristen definiert sind und die Löschungsfristen eingehalten werden,
- wie Gesuche von betroffenen Personen um Auskunft über die eigenen Personendaten und andere datenschutzrechtliche Begehren behandelt werden.

Stichprobenweise kann das Bearbeiten von besonderen Personendaten geprüft werden.

3.2 Organisation und Technik

Vor Ort werden die folgenden Bereiche anhand einer Abgrenzung sowie einer Gewichtung kontrolliert. Diese werden in Zusammenarbeit mit der zu kontrollierenden Stelle definiert:

- Informationssicherheitsstrategie oder Leitlinie zur Informationssicherheit
- Einsatz von Managementsystemen für Informationssicherheit (ISMS) (insbesondere für Schutzstufe S3)
- IT-Sicherheitskonzept (Risikoanalyse, Schutzbedarfsfeststellung, Modellierung, Massnahmenplanung, Umsetzung, Kontrolle der Umsetzung)
- Sicherheits- und Betriebsorganisation (Zuweisung der Verantwortlichkeiten)
- Prozesse und Betrieb der IT (Betriebskonzept sowie -handbücher, insbesondere Back-up-Konzept, Change-Management-Prozess, Incident-Management-Prozess, Sicherheitsmassnahmen, Verschlüsselung, Authentifizierung, Protokollierung und Auswertung bei besonderen Personendaten, Leistungsmessung, Entsorgung von Datenträgern)
- Outsourcing und Cloud Computing (Verträge, SLA, Kontrollmittel, Mandantenfähigkeit, Revision) sowie Prozesse und Betriebe IT (siehe oben)
- Verfügbarkeit der IT-Systeme (Notfallvorsorge, Back-up und Restore)
- Netzwerke (Übersicht Verbindungen, Provider, Anbindung, drahtlose Netzwerke)
- Clients/Server/Drucker/Kopierer (Grundkonfiguration und Verwaltung)
- Regelung des Passwortgebrauchs und technische Umsetzung
- Rollen- und Berechtigungskonzept (Rolle des Datenverantwortlichen, Klassifizierung von Daten, administrative Prozesse bei Zugriffen und Passwörtern (Ein- und Austritt, Mutationen, übergeordnete Rechte)), Umsetzung, Kontrolle von Umfang und Aktualität
- Mobile Arbeitsplätze, Smartphones und mobile Datenträger (Schutzmassnahmen wie kryptografische Massnahmen, Passwort, Patching, Back-up etc., Beschaffung, Bewilligung, Richtlinien, Schulung)
- Weisungen für Benützende (PC/Client, Passwörter, E-Mail und Internet u.a.)
- Planung und Durchführung von Sensibilisierungs- und Schulungsmassnahmen im Bereich IT-Sicherheit (Passwörter, Verwendung von mobilen Geräten, Internet-Dienstleistungen) und Datenschutz
- Intranet- und Internet-Auftritt (Freigabeverfahren der publizierten Inhalte, Schutz der Web-Server und der Dienstleistungen)
- Physische Schutzmassnahmen gegen Umwelteinflüsse sowie Zutrittsrechte

4 Ablauf

4.1 Vor Beginn der Kontrolle einzureichende Unterlagen

Die im Folgenden aufgelisteten Unterlagen sind, wo vorhanden, dem DSB in elektronischer Form einzureichen (via WebTransfer ZH, www.webtransfer.zh.ch).
Es sind keine zusätzlichen Dokumente zu erstellen, sondern nur die bereits vorhandenen Unterlagen in Form von Grundlagen oder Konzepten zusammenzutragen. Der sinnvolle Umfang und Detaillierungsgrad der Dokumentation wird während der Kontrolle vor Ort mit den Verantwortlichen diskutiert.

- Auflistung der externen Stellen (andere Amtsstellen, Kliniken und Spitäler sowie andere Gemeinden usw.) und der gesetzlichen Grundlagen, falls solche auf besondere Personendaten zugreifen
- Übersicht über die Auftragnehmenden im IT-Bereich und ihre Kontaktpersonen
- Aktuelle Verträge mit Auftragnehmenden für IT-Dienstleistungen (Hard- und Software, Netzwerk, Application Service Provider (ASP), Internetauftritt usw.) ohne reine Kauf- und Lizenzverträge. In den Vertragskopien sind die entsprechenden Datenschutzbestimmungen zu markieren.
- Regelungen für die Aufbewahrungsdauer und Löschung der Daten
- Prüfberichte mit Informatikbezug anderer Stellen
- IT-Sicherheitsstrategie oder Leitlinie zur Informationssicherheit
- Dokumentation des Managementsystems für Informationssicherheit (ISMS)
- Dokumentation IT-Sicherheitskonzept (Risikoanalyse, Schutzbedarfsfeststellung, Modellierung, Massnahmenplanung, Umsetzung, Kontrolle der Umsetzung)
- Verzeichnis der Applikationen mit Kurzbeschreibung, Klassifikation der Anwendungen, Schnittstellen sowie Zuweisung der Anwendungs- respektive Datenverantwortlichen
- Verzeichnis der Hardware (Client, Server, Netzwerkkomponenten etc.)
- Verzeichnis der Datenbestände samt Klassifikation
- Sicherheits- und Betriebsorganisation (Zuweisung der Verantwortlichkeiten) in Form von Organigrammen und Stellenbeschreibungen der Verantwortlichen und der Ansprechpartner (IT-Funktionen)
- Weisungen und Anleitungen für Betreiberstellen (Betriebskonzept sowie -handbücher, insbesondere Back-up-Konzept, Protokollierung der Änderungen an IT-Systemen, Change-Management-Prozess, Incident-Management-Prozess, Protokollierung bei besonderen Personendaten, Auswerten von Log-Dateien, Kontrollmechanismen beim Outsourcing, Entsorgung von Datenträgern in den Rollen als interne (IT-Verantwortliche) oder externe Supportstellen, grafische Übersichten der Informatikmittel in der kontrollierten Organisationseinheit in Form von Serverlayouts
- Notfallvorkehrungen in Anlehnung an die Verfügbarkeitsanforderungen

- Dokumentation allfälliger Verschlüsselungstechnologien und deren technischen Umsetzung sowie Schlüsselmanagement
- Dokumentation der technischen Umsetzung der Passwortanforderungen für Systeme und Anwendungen, inklusive Beleg für die Umsetzung (beispielsweise Auszug der Windows Active Directory Group Policy)
- Dokumentation der Massnahmen für Identity- und Accessmanagement (IAM) wie Rollen- und Berechtigungskonzept, Klassifizierung von Daten, administrative Prozesse bei Zugriffen und Passwörtern (Ein- und Austritt, Mutationen, übergeordnete Rechte), Umsetzung, Kontrolle von Umfang und Aktualität, Auswertung von Aufzeichnungen (Logging). Separat sind übergeordnete Rechte von System- und/oder Datenbank-Administratorinnen und -Administratoren, externen Mitarbeitenden und Dienstleistenden oder anderen Stellen (wie Amtsstellen, Spitäler, Kliniken und Gemeinden) zu dokumentieren.
- Netzwerkanbindung (Firewall/DMZ, Zugriffskontrolle zu den Netzwerkressourcen) und Anwendung von drahtlosen Netzwerken, dokumentiert in grafischen Übersichten der Informatikmittel in der kontrollierten Organisationseinheit in Form von Domain- und amtsstelleninternen Netzwerklayouts mit Angabe von externen Netzwerkzugriffen (LEUnet, andere Netzwerkanbindungen, Sicherheitsgateways und eingesetzte Wireless-Geräte)
- Dokumentation für mobile Arbeitsplätze, Smartphones und mobile Datenträger (insbesondere kryptografische Massnahmen bei Daten der Schutzstufe S3): Richtlinien, Bewilligung, geplante und durchgeführte Schulungsmassnahmen
- Beim Intranet- und Internet-Auftritt: Massnahmen zum Schutz der Web-Server und allfälliger Dienstleistungen, Freigabeverfahren der publizierten Inhalte, Privacy Policy (Datenschutzrichtlinie)
- Massnahmen zum physischen Schutz von Informationen wie Zutrittsregelungen und Schutz vor elementaren Bedrohungen (Wasser, Feuer, Rauch, Blitz)
- Benutzerweisungen (PC/Client, Passwörter, E-Mail und Internet, mobile Arbeitsplätze und Geräte, WLAN u.a.)
- Dokumentation der Planung und Durchführung von Sensibilisierungs- und Schulungsmassnahmen im Bereich IT-Sicherheit (Passwörter, Verwendung von mobilen Geräten, E-Mail und Internet-Dienstleistungen) sowie Datenschutz

4.2 Prüfung der eingereichten Unterlagen

Der Datenschutzreview beginnt mit einer Überprüfung und Beurteilung der eingereichten Unterlagen durch den DSB.

4.3 Vorbesprechung der Kontrolle vor Ort

Mit der Leiterin oder dem Leiter der kontrollierten Stelle und der Ansprechperson (meistens die Verantwortliche respektive der Verantwortliche IT-Betrieb), dem DSB und, falls nötig, mit weiteren Mitarbeitenden oder den externen Auftragnehmenden wird eine kurze Vorbesprechung zu Beginn der Kontrolle vor Ort geführt, um

- über die bereits erfolgten Schritte (Status der geprüften Dokumentation) und den weiteren Ablauf sowie noch offene Punkte zu informieren,
- über den Einsatz des System-, Netz- oder Webscanners zu informieren,
- den Zeitplan der Kontrolle vor Ort zu fixieren,
- allfällige Fragen zu beantworten.

4.4 Überprüfung mit System-, Netz- und Webscanner

Die Systeme, das Netzwerk und die Webdienste können mit einem System- und Netzscanner (GFI LanGuard) oder einem Webscanner (Netsparker) automatisiert auf Schwachstellen überprüft werden. Der DSB haftet gemäss kantonalem Haftungsgesetz, sollten während eines Datenschutzreviews durch den Einsatz dieser Instrumente Schäden entstehen.

4.5 Kontrolle vor Ort

Die Kontrolle vor Ort beinhaltet die Klärung der offenen Punkte. Dies geschieht durch das Führen von Interviews, der Vornahme von Stichproben sowie dem Einsatz von Prüfsoftware. Jeder Arbeitstag wird mit einem kurzen Statusmeeting beendet.

4.6 Schlussbesprechung

Die Schlussbesprechung dient dem Vorstellen und Erläutern des Berichtentwurfs und der Klärung offener Fragen.

4.7 Bericht

Der DSB erstellt in der Regel innert Monatsfrist nach der Kontrolle einen Bericht. Der Bericht enthält das Ergebnis, den Umfang und Inhalt der Kontrolle, die Abgrenzungen und die Gewichtung sowie, falls nötig, priorisierte Massnahmen zur Umsetzung sowie eine Stellungnahme des geprüften Organs zur Umsetzung. Je ein Exemplar des Berichts wird der kontrollierten Stelle und bei Gemeinden zusätzlich dem Bezirksrat zugestellt.

4.8 Umsetzung der Massnahmen

Die kontrollierte Stelle informiert den DSB über die Umsetzung der mit einer Frist versehenen Massnahmen.

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh