dsb
datenschutzbeauftragter
kanton zürich

Ziele, Umfang, Ablauf Datenschutzreview

Inhalt

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 Informationssicherheit.

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. Der DSB und seine Mitarbeitenden sind 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 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,
- wie der Datenschutz und die Informationssicherheit in Verträgen zwischen Auftraggebenden und Auftragnehmenden, die bei ihrer Leistungserbringung potenziell Zugang zu Personendaten haben, gewährleistet sind.

Stichprobenweise kann das Bearbeiten von besonderen Personendaten geprüft werden.

3.2 Organisation und Technik

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

- Informationssicherheitsstrategie oder Leitlinie zur Informationssicherheit
- Prozesse und Verfahren für die systematische Verwaltung der Informationssicherheit, Einsatz eines Informationssicherheits-Managementsystems (ISMS) (insbesondere für Schutzstufe S3)
- Informationssicherheitskonzept (Risikoanalyse, Schutzbedarfsfeststellung, Modellierung, Massnahmenplanung, Umsetzung, Kontrolle der Umsetzung, regelmässige Überprüfung der Informationssicherheit)
- Sicherheits- und Betriebsorganisation (Zuweisung der Verantwortlichkeiten)
- Weisungen für Benutzerinnen und Benutzer (PC / Client, Passwörter, E-Mail und Internet)
- Planung und Durchführung von Sensibilisierungs- und Schulungsmassnahmen im Bereich Datenschutz und Informationssicherheit (Passwörter, Verwendung von mobilen Geräten, Internet-Dienstleistungen)
- Outsourcing inklusive Cloud Computing (Verträge, SLA, Kontrollmittel, Mandantenfähigkeit, Revision) sowie Prozesse und Betrieb IT
- Dokumentation und Inventar der Applikationen und Infrastrukturkomponenten inklusive der Datenbestände und deren Klassifizierung
- Rollen- und Berechtigungskonzept (Rolle des Datenverantwortlichen, administrative Prozesse bei Zugriffen und Passwörtern (Ein- und Austritt, Mutationen, übergeordnete Rechte)), Umsetzung, Kontrolle von Umfang und Aktualität
- Regelung des Passwortgebrauchs und technische Umsetzung
- Prozesse und Betrieb der IT (Betriebskonzept sowie -handbücher, insbesondere Back-up-Konzept, Change-Management-Prozess, Incident-Management-Prozess, Capacity-Management-Prozess, Vulnerability-Management-Prozess, Patch-Management-Prozess, Sicherheitsmassnahmen, Verschlüsselung, Authentifizierung, Life-Cycle-Management-Prozess, Protokollierung und Auswertung bei besonderen Personendaten, Leistungsmessung, Entsorgung von Datenträgern)
- Clients / Server / Drucker / Kopierer (Grundkonfiguration / IT-Grundschutz und -Verwaltung)
- Netzwerke und Sicherheitsgateways inklusive der Netzwerkarchitektur (Vorgaben, Prozesse, Übersicht Verbindungen, Provider, Anbindung, drahtlose Netzwerke)
- Telefonie- und Kommunikationslösungen (Voice-over-IP / VOIP, Unified Communication and Colaboration / UCC)
- Mobile Arbeitsplätze, Smartphones und mobile Datenträger (Schutzmassnahmen wie kryptografische Massnahmen, Passwort, Patching, Back-up usw., Beschaffung, Bewilligung, Richtlinien, Schulung)
- Verfügbarkeit und Notfallvorsorge der IT-Systeme und -Applikationen (Hochverfügbarkeit, Business Continuity Management, Disaster Recovery, Back-up und Restore)
- Physische Schutzmassnahmen gegen Umwelteinflüsse sowie Zutrittsrechte

4 Ablauf

4.1 Vorbesprechung der Kontrolle vor Ort

Mit der Leiterin oder dem Leiter der kontrollierten Stelle und den Ansprechpersonen (meistens die Verantwortlichen des IT-Betriebs), 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- und Netzwerkscanners (GFI Languard o.ä.) oder des Webscanners (Netsparker o.ä.) zu informieren,
- den Zeitplan der Kontrolle vor Ort zu fixieren,
- allfällige Fragen zu beantworten.

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

4.2 Einzureichende Unterlagen

Die Unterlagen sind, wo vorhanden, dem DSB in elektronischer Form einzureichen (via Web-Transfer ZH, https://webtransfer.zh.ch).

Es müssen keine zusätzlichen Dokumente erstellt, sondern nur die bereits vorhandenen Unterlagen in Form von Grundlagen oder Konzepten zusammengetragen werden.

- Auflistung der externen Stellen (andere Amtsstellen, Kliniken und Spitäler sowie andere Gemeinden usw.) und der gesetzlichen Grundlagen, falls diese auf besondere Personendaten zugreifen
- Übersicht über die Auftragnehmenden im IT-Bereich
- 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 Datenschutzbestimmungen zu markieren.
- Regelungen für die Aufbewahrungsdauer und die Vernichtung der Daten
- Berichte durchgeführter Überprüfungen der Informationssicherheit (inklusive Berichte kantonaler oder externer Prüf- und Revisionsstellen oder Auszüge davon)
- Informationssicherheitsstrategie oder Leitlinie zur Informationssicherheit
- Dokumentation der Prozesse und Verfahren für die systematische Verwaltung der Informationssicherheit oder des Informationssicherheits-Managementsystems (ISMS)
- Dokumentation des Informationssicherheitskonzepts (Risikoanalyse, Schutzbedarfsfeststellung, Modellierung, Massnahmenplanung, Umsetzung, Kontrolle der Umsetzung)
- Sicherheits- und Betriebsorganisation (Zuweisung der Verantwortlichkeiten) in Form von Organigrammen und allenfalls Funktionsbeschreibungen der Verantwortlichen und der Ansprechpartner (IT-Funktionen)

- Weisungen für Benutzerinnen und Benutzer (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 Datenschutz und Informationssicherheit (Passwörter, Verwendung von mobilen Geräten, E-Mail und Internet-Dienstleistungen)
- Verzeichnis der Datenbestände samt Klassifikation
- Verzeichnis der Applikationen mit Kurzbeschreibung, Klassifikation der Anwendungen, Schnittstellen sowie Zuweisung der Anwendungs- respektive Datenverantwortlichen
- Dokumentation des Inventarprozesses der Infrastrukturkomponenten inklusive Inventarliste (Client, Server, Netzwerkkomponenten usw.)
- Dokumentation der Massnahmen für Identity- und Accessmanagement (IAM) wie Rollen- und Berechtigungskonzept, administrative Prozesse bei Zugriffen und Passwörtern (Ein- und Austritt, Mutationen, übergeordnete Rechte), Umsetzung, Kontrolle von Umfang und Aktualität, Auswertung von Aufzeichnungen (Logging). Übergeordnete Rechte von System- und/oder Datenbank-Administratorinnen und -Administratoren, externen Mitarbeitenden und Dienstleistenden oder anderen Stellen sind separat zu dokumentieren (wie Amtsstellen, Spitäler, Kliniken und Gemeinden).
- Dokumentation der technischen Umsetzung der Passwortanforderungen für Systeme und Anwendungen, inklusive Beleg für die Umsetzung (beispielsweise Auszug der Windows Active Directory Group Policy)
- Weisungen und Anleitungen für Betreiberstellen (Betriebskonzept sowie -handbücher, insbesondere Back-up-Konzept, Protokollierung der Änderungen an IT-Systemen, Change-Management-Prozess, Incident-Management-Prozess, Capacity-Management-Prozess, Vulnerability-Management-Prozess, Patch-Management-Prozess, Life-Cycle-Management-Prozess, Protokollierung bei besonderen Personendaten, Auswerten von Log-Dateien, Kontrollmechanismen beim Outsourcing, Entsorgung von Datenträgern, grafische Übersichten der Informatikmittel in der kontrollierten Organisationseinheit in Form von Serverlayouts)
- 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 (andere Netzwerkanbindungen, Sicherheitsgateways und eingesetzte Wireless-Geräte)
- Weisungen, Unterlagen und Dokumente zur Telefonie- und Kommunikationslösung (Voice-over-IP / VOIP, Unified Communication and Collaboration / UCC) sowie implementierte Schutzmassnahmen
- Dokumentation allfälliger Verschlüsselungstechnologien und deren technischen Umsetzung sowie Schlüsselmanagement
- Dokumentation für mobile Arbeitsplätze, Smartphones und mobile Datenträger (insbesondere kryptografische Massnahmen bei Daten der Schutzstufe S3): Richtlinien, Bewilligung, geplante und durchgeführte Schulungsmassnahmen
- Dokumentation des Business-Continuity-Managements und der Notfallvorkehrungen in Anlehnung an die Verfügbarkeitsanforderungen
- Massnahmen zum physischen Schutz von Informationen wie Zutrittsregelungen und Schutz vor elementaren Bedrohungen (Wasser, Feuer, Rauch, Blitz)

4.3 Prüfung der eingereichten Unterlagen

Der Datenschutzbeauftragte prüft und beurteilt die eingereichten Unterlagen vor der Prüfung vor Ort.

4.4 Prüfung vor Ort

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

4.5 Berichtsentwurf und Schlussbesprechung

Nach Konsolidierung der vorliegenden Informationen wird der Berichtsentwurf erstellt und der geprüften Einheit vor der Schlussbesprechung zugestellt.

Der Berichtsentwurf wird in der Schlussbesprechung erläutert, worauf offene Fragen geklärt und die Umsetzungstermine bestätigt werden.

4.6 Stellungnahme zur Umsetzung

Nach der Schlussbesprechung erhält die kontrollierte Stelle die Gelegenheit, zur Umsetzung der Massnahmen schriftlich Stellung zu nehmen.

4.7 Bericht

Nach dem Eintreffen der Stellungnahme des geprüften Organs verfasst der DSB den finalen Bericht. Dieser enthält das Ergebnis, den Umfang und Inhalt der Kontrolle, die Abgrenzungen und die Gewichtung sowie, falls nötig, priorisierte Massnahmen sowie als Beilage die Stellungnahme des geprüften Organs zur Umsetzung. Je ein Exemplar des Berichts wird dem geprüften Organ und bei Gemeinden zusätzlich dem Bezirksrat zugestellt.

4.8 Umsetzung der Massnahmen

Das geprüfte Organ informiert den DSB zeitnah 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