

Datenschutzbeauftragter
des Kantons Zürich
Postfach, CH-8090 Zürich

Tel.: 043 259 39 99
Fax: 043 259 51 38

datenschutz@dsb.zh.ch
www.datenschutz.ch

Ziele, Umfang und Ablauf

Ablauf Datenschutzreview



Datenschutz
mit Qualität

Inhalt

1. Ziele des Datenschutzreviews	3
2. Gesetzliche Grundlagen	3
3. Umfang und Inhalt der Kontrolle	3
3.1 Recht	3
3.2 Organisation und Technik	4
4. Ablauf	5
4.1 Vor Beginn der Kontrolle einzureichende Unterlagen	5
4.2 Prüfung der eingereichten Unterlagen	6
4.3 Vorgesprechung der Kontrolle vor Ort.....	7
4.4 Kontrolle vor Ort.....	7
4.5 Schlussbesprechung	7
4.6 Bericht.....	7
4.7 Umsetzung der Massnahmen	7

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 Informations- und Kommunikationstechnologie (IKT).

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 potentiell Zugang zu Personendaten haben, der Datenschutz durch die Verträge gewährleistet wird
- ob für besondere Personendaten die Aufbewahrungsfristen definiert sind und die Lösungsfristen eingehalten 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:

- IKT-Sicherheitsstrategie oder Leitlinie zur Informationssicherheit
- Einsatz von Managementsystemen für Informationssicherheit (ISMS) (insbesondere für Schutzstufe S3)
- IKT-Konzept (Schutzbedarfsfeststellung, Modellierung, Massnahmenplanung, Umsetzung, Kontrolle der Umsetzung)
- Sicherheits- und Betriebsorganisation (Zuweisung der Verantwortlichkeiten)
- Weisungen für Benützer (PC/Client, Passwörter, E-Mail und Internet)
- Weisungen für Betreibende (Betriebskonzept sowie Betriebshandbücher, insbesondere Backup-Konzept, Protokollierung der Änderungen an IKT-Systemen, Protokollierung bei besonderen Personendaten, Auswerten von Log-Dateien, Kontrollmechanismen beim Outsourcing, Entsorgung von Datenträgern)
- Planung und Durchführung von Sensibilisierungs- und Schulungsmassnahmen im Bereich IKT-Sicherheit (Passwörter, Verwendung von mobilen Geräten, Internet-Dienstleistungen) und Datenschutz
- 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]
- Netzwerkanbindung (Firewall/DMZ, Zugriffskontrolle zu den Netzwerkressourcen) und Anwendung von drahtlosen Netzwerken
- Mobile Arbeitsplätze, Smartphones und mobile Datenträger (insbesondere kryptografische Massnahmen bei Daten der Schutzstufe S3): Richtlinien, Bewilligung, Schulung
- Intranet- und Internet-Auftritt (Freigabeverfahren der publizierten Inhalte, Schutz der Web-Server und der Dienstleistungen)

4. Ablauf

4.1 Vor Beginn der Kontrolle einzureichende Unterlagen

Die im Folgenden aufgelisteten Unterlagen sind dem DSB in Papier- oder in elektronischer Form einzureichen.

Es sind keine zusätzlichen Dokumente zu erstellen, sondern es sind 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 Auftragnehmer im IKT-Bereich und ihre Kontaktpersonen
- Aktuelle Verträge mit Auftragnehmern für IKT-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
- IKT-Sicherheitsstrategie oder Leitlinie zur Informationssicherheit
- Dokumentation des Managementsystems für Informationssicherheit (ISMS)
- Dokumentation IKT-Konzept (Schutzbedarfsfeststellung, Modellierung, Massnahmenplanung, Umsetzung, Kontrolle der Umsetzung)
- Verzeichnis der Applikationen mit Kurzbeschreibung, Klassifikation der Anwendungen und Zuweisung der Anwendungs- respektive Datenverantwortlichen
- Sicherheits- und Betriebsorganisation (Zuweisung der Verantwortlichkeiten) in Form von Organigrammen und Stellenbeschreibungen der Verantwortlichen und der Ansprechpartner (IKT-Funktionen)
- Benutzerweisungen (PC/Client, Passwörter, E-Mail und Internet, Mobile Arbeitsplätze und Geräte)
- Weisungen und Anleitungen für Betreiberstellen (Betriebskonzept sowie Betriebshandbücher, insbesondere Backup-Konzept, Protokollierung der Änderungen an IKT-Systemen, Protokollierung bei besonderen Personendaten, Auswerten von Log-Dateien, Kontrollmechanismen beim Outsourcing, Entsorgung von Datenträgern in den Rollen als interne (IKT-Verantwortliche) oder externe Sup-

portstellen, grafische Übersichten der Informatikmittel in der kontrollierten Organisationseinheit in Form von Serverlayouts

- Dokumentation der Planung und Durchführung von Sensibilisierungs- und Schulungsmassnahmen im Bereich IKT-Sicherheit (Passwörter, Verwendung von mobilen Geräten, E-Mail und Internet-Dienstleistungen) sowie Datenschutz
- Dokumentation der technischen Umsetzung der Passwortanforderungen für Systeme und Anwendungen
- Dokumentation der Massnahmen für Identity- und Accessmanagement (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-Administratoren, externen Mitarbeitern 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), Weisungen an Benutzer und Massnahmenpläne
- 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)

4.2 Prüfung der eingereichten Unterlagen

Der Datenschutzreview beginnt mit einer Überprüfung der Angaben im Reviewtool (Systemanalyse, Fragebogen mit rechtlichen, organisatorischen und technischen Fragen) und der eingereichten Unterlagen.

4.3 Vorbereitung der Kontrolle vor Ort

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

- über die bereits erfolgten Schritte (Auswertung Fragebogen aus dem Review-Tool und Status der geprüften Dokumentation) und den weiteren Ablauf zu informieren
- den Zeitplan der Kontrolle vor Ort zu fixieren
- allfällige Fragen zu beantworten

4.4 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 Prüf-Software. Jeder Arbeitstag wird mit einem kurzen Statusmeeting beendet.

4.5 Schlussbesprechung

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

4.6 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. Je ein Exemplar des Berichts wird der geprüften Stelle und bei Gemeinden zusätzlich dem Bezirksrat zugestellt.

4.7 Umsetzung der Massnahmen

Die kontrollierte Stelle informiert den DSB über die mit einer hohen Priorität versehenen und innerhalb der vereinbarten Frist umgesetzten Massnahmen.