



**dsb**

datenschutzbeauftragte  
des kantons zürich

---

# Ziele, Umfang, Ablauf Datenschutzreview

## Inhalt

<b>1</b>	<b>Ziele des Datenschutzreviews</b>	<b>2</b>
<b>2</b>	<b>Gesetzliche Grundlagen</b>	<b>2</b>
<b>3</b>	<b>Umfang und Inhalt der Kontrolle</b>	<b>2</b>
3.1	Recht .....	2
3.2	Organisation und Technik .....	2
<b>4</b>	<b>Ablauf</b>	<b>3</b>
4.1	Vorbesprechung der Kontrolle vor Ort .....	3
4.2	Einzureichende Unterlagen .....	3
4.3	Prüfung der eingereichten Unterlagen .....	4
4.4	Prüfung vor Ort.....	5
4.5	Berichtsentwurf und Schlussbesprechung.....	5
4.6	Bericht.....	5
4.7	Umsetzung der Massnahmen.....	5

## 1 Ziele des Datenschutzreviews

Im Rahmen des Datenschutzreviews kontrolliert die Datenschutzbeauftragte (DSB) die Umsetzung der rechtlichen, organisatorischen und technischen Aspekte mittels der eingereichten Unterlagen und der vor Ort vorzufindenden Massnahmen.

Zusätzlich bewirkt die Kontrolle eine Sensibilisierung in Bezug auf einen wirksamen Datenschutz und eine angemessene Informationssicherheit.

## 2 Gesetzliche Grundlagen

Die DSB überwacht die Anwendung der Vorschriften über den Datenschutz (§ 34 lit. c i.V.m. § 35 Gesetz über die Information und den Datenschutz, IDG, LS 170.4). Sie 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 ihre 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 der DSB werden durch eine entsprechende Schweigepflicht abgesichert. Die DSB und ihre 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 für Personendaten die Aufbewahrungsfristen definiert sind und die Lösungsfristen eingehalten 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 Datenbearbeitung) 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 Daten mit erhöhtem Schutzbedarf)
- 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)
- Verträge, SLA, Kontrollmittel, Mandantenfähigkeit, Revision
- 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 Backup-Konzept, Change-Management-Prozess, Incident-Management-Prozess, Vulnerability-Management-Prozess, Patch-Management-Prozess, Sicherheitsmassnahmen, Verschlüsselung, Authentifizierung, Protokollierung und Auswertung bei besonderen Personendaten, 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)
- Mobile Arbeitsplätze, Smartphones und mobile Datenträger (Schutzmassnahmen wie kryptografische Massnahmen, Passwort, Patching, Backup usw., Beschaffung, Bewilligung, Richtlinien, Schulung)
- Verfügbarkeit der IT-Systeme und -Applikationen (Backup und Restore)
- Physische Schutzmassnahmen gegen Umwelteinflüsse sowie Zutrittsrechte

## 4 Ablauf

### 4.1 Vorbereitung der Kontrolle vor Ort

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

### 4.2 Einzulegende Unterlagen

Die Unterlagen sind, wo vorhanden, der DSB in elektronischer Form einzulegen (via Web-Transfer ZH, [webtransfer.zh.ch](http://webtransfer.zh.ch)).

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

1. Auflistung der externen Stellen (andere Amtsstellen, Kliniken und Spitäler sowie andere Gemeinden usw.) und der gesetzlichen Grundlagen, falls diese auf besondere Personendaten zugreifen
2. Übersicht über die Auftragnehmenden im IT-Bereich
3. Auflistung aktueller Verträge mit Auftragnehmenden für IT-Dienstleistungen (Hard- und Software, Netzwerk, Application Service Provider (ASP), Internetauftritt usw.) ohne reine Kauf- und Lizenzverträge. Die Auflistung hat eine Angabe zum Inhalt der Vertragsbeziehung zu enthalten. Es sind die Vertragsbeziehungen zu markieren, in deren Erfüllung Personendaten durch die Auftragnehmenden bearbeitet werden. Die DSB nimmt eine Stichprobe der Liste und verlangt die Einreichung der Vertragskopien. In den Vertragskopien sind die Datenschutzbestimmungen zu markieren.
4. Regelungen für die Aufbewahrungsdauer und die Vernichtung der Daten
5. Berichte durchgeführter Überprüfungen der Informationssicherheit (inklusive Berichte kantonaler oder externer Prüf- und Revisionsstellen oder Auszüge davon)
6. Informationssicherheitsstrategie oder Leitlinie zur Informationssicherheit
7. Dokumentation der Prozesse und Verfahren für die systematische Verwaltung der Informationssicherheit oder des Informationssicherheits-Managementsystems (ISMS)

8. Dokumentation des Informationssicherheitskonzepts (Risikoanalyse, Schutzbedarfs-feststellung, Modellierung, Massnahmenplanung, Umsetzung, Kontrolle der Umsetzung)
9. Sicherheits- und Betriebsorganisation (Zuweisung der Verantwortlichkeiten) in Form von Organigrammen und allenfalls Funktionsbeschreibungen der Verantwortlichen und der Ansprechpartner (IT-Funktionen)
10. Weisungen für Benutzerinnen und Benutzer (PC / Client, Passwörter, E-Mail und Internet, mobile Arbeitsplätze und Geräte, WLAN u.a.)
11. Dokumentation der Planung und Durchführung von Sensibilisierungs- und Schulungsmassnahmen im Bereich Datenschutz und Informationssicherheit (Passwörter, Verwendung von mobilen Geräten, E-Mail und Internet-Dienstleistungen)
12. Verzeichnis der Datenbestände samt Klassifikation
13. Verzeichnis der Applikationen mit Kurzbeschreibung, Klassifikation der Anwendungen, Schnittstellen sowie Zuweisung der Anwendungs- respektive Datenverantwortlichen
14. Dokumentation des Inventarprozesses der Infrastrukturkomponenten inklusive Inventarliste (Client, Server, Netzwerkkomponenten usw.)
15. 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).
16. Dokumentation der technischen Umsetzung der Passwortanforderungen für Systeme und Anwendungen, inklusive Beleg für die Umsetzung (beispielsweise Auszug der Windows Active Directory Group Policy)
17. Dokumentation der technischen Umsetzung der Datenschutz- und Informationssicherheitseinstellungen für Systeme und Anwendungen, inklusive Beleg für die Umsetzung (beispielsweise Auszug der Windows Active Directory Group Policy für Telemetrie, Windows Firewall usw.)
18. Weisungen und Anleitungen für Betreiberstellen (Betriebskonzept sowie -handbücher, insbesondere Backup-Konzept, Protokollierung der Änderungen an IT-Systemen, Change-Management-Prozess, Incident-Management-Prozess, Vulnerability-Management-Prozess, Patch-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)
19. 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)
20. Dokumentation allfälliger Verschlüsselungstechnologien und deren technischen Umsetzung sowie Schlüsselmanagement
21. Dokumentation für mobile Arbeitsplätze, Smartphones und mobile Datenträger: Kryptografische Massnahmen, Richtlinien, Bewilligung, geplante und durchgeführte Schulungsmassnahmen
22. Dokumentation des Business-Continuity-Managements und der Notfallvorkehrungen in Anlehnung an die Verfügbarkeitsanforderungen
23. Massnahmen zum physischen Schutz von Informationen wie Zutrittsregelungen und Schutz vor elementaren Bedrohungen (Wasser, Feuer, Rauch, Blitz)

#### 4.3 Prüfung der eingereichten Unterlagen

Die DSB 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.

In der Schlussbesprechung wird der Berichtsentwurf erläutert, offene Fragen geklärt und die Umsetzungstermine bestätigt.

#### **4.6 Bericht**

Nach der Schlussbesprechung bestätigt das geprüfte Organ die inhaltliche Korrektheit des Berichts und die DSB fasst den finalen Bericht. Dieser enthält das Ergebnis, den Umfang und Inhalt der Kontrolle, die Abgrenzungen und die Gewichtung sowie, falls nötig, priorisierte Massnahmen. Je ein Exemplar des Berichts wird dem geprüften Organ und bei Gemeinden zusätzlich dem Bezirksrat zugestellt.

#### **4.7 Umsetzung der Massnahmen**

Das geprüfte Organ informiert die DSB zeitnah über die Umsetzung der mit einer Frist versehenen Massnahmen.