

Tätigkeitsbericht 2015

**des Datenschutzbeauftragten der Stadt Winterthur
an den Grossen Gemeinderat der Stadt Winterthur**

Berichtsperiode vom 1. Januar 2015 bis zum 31. Dezember 2015

Inhaltsverzeichnis

1. Das Berichtsjahr in Kürze	3
2. Ausgewählte Dossiers	3
2.1 Glasfasernetz Winterthur	3
2.2 Bewohnerrufanlage Alterszentrum Adlergarten	5
2.3 Elektronisches Bewerbungsmanagement	6
3. Öffentlichkeitsarbeit	7
3.1 Interview zum Thema Datensicherheit an Schulen	7
4. Internes	8
4.1 Zusammenarbeit mit anderen Datenschutzbehörden	8
5. Ausblick	9
6. Anhang	10
6.1 Thematische Übersicht	10
6.2 Bearbeitungsstand der Dossiers per 31. Dezember 2015	11
6.3 Aufschlüsselung der Neueingänge nach Aufgaben gemäss § 34 IDG	11

§ 39 Informations- und Datenschutzgesetz des Kantons Zürich (IDG)

Der oder die Beauftragte berichtet dem Wahlorgan periodisch über Umfang und Schwerpunkt der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes. Der Bericht wird veröffentlicht.

§ 10 Verordnung über den oder die Datenschutzbeauftragte/n der Stadt Winterthur

Der oder die Datenschutzbeauftragte erstattet dem Grossen Gemeinderat jährlich Bericht über seine bzw. ihre Tätigkeit.

1. Das Berichtsjahr in Kürze

Im zweiten Jahr in Folge verzeichnete die Datenaufsicht einen leichten Rückgang der eingegangenen Anfragen, wenn auch die bisher tiefste Anzahl aus dem Jahr 2012 nicht erreicht wurde. Der Datenschutzbeauftragte konnte daher einige ältere Dossiers erledigen und verhindern, dass die Anzahl der pendenten Fälle erneut anstieg. Allerdings sind die Zahlen nach wie vor höher, als anlässlich der Schaffung der Datenaufsicht vor nunmehr fünf Jahren prognostiziert.

Die Vielfalt der Fälle erstaunt nach wie vor, die Palette reicht von der Prüfung von Ausnahmen für den städtischen Contentfilter, die Sicherung von Routern im Superblock über diverse Einsichtsrechte in den Bereichen Polizei, Schule, Finanzverwaltung oder Personalerhebung, die Nutzung von Daten über ältere Gebäude, Geoinformationsdaten, die Ortung von Mitarbeitern, bis hin zu falschen Mailverteilern oder falsch eingerichteten Zugriffsrechten auf älteren Systemen. Eine thematische Übersicht der eingegangenen Fälle findet sich im Anhang.

Von der Art der Anfragen her zeigt sich ein erfreulicher Trend, die Datenaufsichtsstelle früher in Projekte und Prozessabläufe einzubeziehen. Dadurch verlagerte sich ein Teil der Tätigkeit von Vorabkontrollen hin zu der Bewertung einzelner datenrelevanter Aspekte. Da hierdurch in Fällen, die einer gesetzlichen Vorabkontrolle bedurften, die entsprechenden Risiken frühzeitig gemindert werden konnten, fiel der Aufwand für die spätere, eigentliche Vorabkontrolle im Durchschnitt bedeutend geringer aus. Dies brachte eine Entlastung für alle Beteiligten Stellen, sowie für private Projektpartner.

2. Ausgewählte Dossiers

2.1 Glasfasernetz Winterthur

Im Frühjahr 2013 wurde die Datenaufsicht erstmals auf den Aufbau des städtischen Glasfasernetzes aufmerksam. Die Stadtwerke erkundigten sich, welche Daten für die Erschliessung der einzelnen Liegenschaften verwendet werden dürften und was hierbei zu beachten wäre. Im Einzelnen handelte es sich zunächst um Datensätze Geoinformationsdatenbank, die dazu verwendet wurden, Verträge (sog. Hausanschlussverträge) mit den Grundstückseigentümern abzuschliessen. Hierbei wurden Name und Adresse der Eigentümer der neu angeschlossenen Liegenschaften an die Stadtwerke bekannt gegeben.

Die Bekanntgabe dieser Daten erachtete die Datenaufsicht als unproblematisch, da es sich bei den Eigentümerdaten um Daten handelte, die im Rahmen des Grundbuches grundsätzlich öffentlich sind. Insbesondere aber stützte sich die Bereitstellung des Glasfasernetzes auf einen deutlichen Abstimmungsentscheid der Bürgerinnen und Bürger von Winterthur vom 25. November 2012, der den Stadtwerken einen klaren Auftrag zur Bereitstellung dieser neuen Infrastruktur gab. Im Hinblick auf die Rechtslage gab die Datenaufsicht den Stadtwerken einige Vorgaben bezüglich der Verwendung und späteren Löschung der erhaltenen Eigentümerdaten, die eine spätere Zweckänderung ausschlossen.

In der Folge gelangten die Stadtwerke erneut an die Datenaufsicht. Nach Fertigstellen des Netzes sollten private Anbieter die Möglichkeit erhalten, die Bewohnerinnen und Bewohner der neu erschlossenen Liegenschaften auf ihre Telekommunikationsangebote aufmerksam zu machen. Zu diesem Zweck sollten sie aktualisierte Listen erhalten, welche die Stadtwerke wiederum aus Listen der Datenbank der Einwohnerkontrolle zusammenstellen würden.

Als Grundlage für die Zusammenarbeit mit den privaten Anbietern von Internetdienstleistungen wurde der Abstimmungsentscheid vom November 2012 angeführt. In den Abstimmungsunterlagen legte der Stadtrat dar, dass dieses Netz in Zusammenarbeit mit Swisscom aufgebaut werde und dass die vertraglichen Vereinbarungen mit Swisscom den Empfehlungen der Eidgenössischen Kommunikationskommission und der Wettbewerbskommission folgten. Auf der Grundlage dieser Vereinbarung stünden zwei der vier Faserleitungen Drittanbietern zur Verfügung.

Für die Datenaufsicht war entscheidend, dass die Bevölkerung neben der Vergabe des Kredits der Partnerschaft mit der Swisscom zugestimmt hatte. Damit erteilten die Stimmbürgerinnen und Stimmbürger den Stadtwerken implizit den (durch das Wettbewerbsrecht vorgegebenen) Auftrag, das Glasfasernetz Drittanbietern als Plattform anzubieten, und – soweit möglich – eine wirtschaftliche Gleichbehandlung mit der Swisscom sicherzustellen. In diesem Licht betrachtet erschien die Weitergabe der Kontaktadressen der neu erschlossenen Liegenschaften als eine vertretbare Lösung. Die Rechte der Betroffenen wurden durch vertragliche Vereinbarung mit den betreffenden Firmen abgesichert. Diese verbieten ausdrücklich eine andere Verwendung als zur Bewerbung des eigenen Produktes in Bezug auf die Nutzung des städtischen Glasfasernetzes.

Seit Beginn des „Rollouts“ des Glasfasernetzes haben sich einige der kontaktierten Bewohnerinnen und Bewohner gemeldet, die keine derartige Werbung wünschen. Es zeigte sich, dass die Aufbereitungsprozesse der Kontaktlisten auf dem Papier bestanden, in der Praxis jedoch noch erheblich angepasst und verfeinert werden mussten. Die Datenaufsicht konnte schliesslich feststellen, dass die Kommunikation

zwischen Personen, die keine Glasfaserwerbung wünschen, den Stadtwerken als Plattformanbieter und den Anbieterfirmen als externe Bearbeiter der Adressen nunmehr funktioniert.

2.2 Bewohnerrufanlage Alterszentrum Adlergarten

Die Datenaufsicht wurde angefragt, welche rechtlichen Vorgaben bei der Einrichtung einer Bewohnerrufanlage zu beachten seien. Das Projekt sah vor, dass sowohl die Bewohner, als auch das Personal einen Rufsender auf sich tragen würden, der zugleich eine Ortung ermöglicht. Über ein Computersystem könnte sodann in einem Notfall jenes Personal alarmiert werden, das sich gerade in der Nähe befindet. Bei der Prüfung des Konzeptes sowie der im Entwurf vorliegenden Merkblätter und Einwilligungserklärungen identifizierte die Datenaufsicht mehrere Punkte, die aus rechtlicher Sicht heikel erschienen.

In Bezug auf das Personal stützte sich die Pflicht, einen Rufsender auf sich zu tragen, auf das Weisungsrecht des Personalrechts sowie auf § 24 VVO PST¹, der die Aufzeichnung und Auswertung von Daten bei der Benützung von technischen Einrichtungen ermöglicht. Da der Zweck des Rufsenders nicht in der Überwachung des Personals liegt, sondern darin, in Notfällen eine möglichst kurze Reaktionszeit sicherzustellen, bewertete die Datenaufsicht diese Rechtsgrundlage grundsätzlich als genügend.

Allerdings musste gemäss § 24 Abs. 3 VVO PST sichergestellt werden, dass die durch das System aufgezeichneten Daten nicht zu Zwecken der Überwachung und Kontrolle des Personals verwendet würden. Dabei zeigte sich eine technische Schwierigkeit, da der Hersteller der Software zur Betreibung der Rufanlage mitteilte, die feste Speicherdauer von 30 Tagen (!) könne nicht angepasst werden.

Die Datenaufsicht einigte sich in der Folge mit der zuständigen Stelle, die technischen Defizite der Anlage durch organisatorische Vorkehrungen, rechtliche Vorschriften und spezifische Geheimhaltungserklärungen der Mitarbeiterinnen und Mitarbeiter einzufangen. Dazu wurden die Nutzungszwecke und Prozessabläufe der Anlage, die berechtigten Personen sowie der Umgang mit den gespeicherten Daten geregelt. Zusätzlich wurde ein Reglement über die Aufzeichnung von Daten der Bewohnerrufanlage im Alterszentrum Adlergarten erstellt, das auf der einen Seite den zulässigen Zweck der Anlage präziser fasste und auf der anderen Seite die Nachverfolgung von Mitarbeitenden, die Verwendung der Aufzeichnungen für andere Zwecke als zur Fehleranalyse sowie die Weitergabe der Aufzeichnungen für unzulässig erklärt.

¹ Vollzugsverordnung zum Personalstatut vom 9. Juni 1999.

In Bezug auf die Bewohnerinnen und Bewohner des Alterszentrums waren sodann zwei unterschiedliche Szenarien zu prüfen. Unter normalen Bedingungen würde ihnen frei stehen, einen Rufsender zu tragen oder nicht.

Unter gewissen Bedingungen sollten die Rufsender zudem eingesetzt werden, um einen Alarm auszulösen, wenn die Trägerin oder der Träger einen vorher definierten Perimeter verlässt. Damit sollte verhindert werden, dass »weglaufgefährdete« Personen irgendwo ausserhalb der Residenz durch die Strassen irrten und dabei beispielsweise Gefahr liefen, einen Unfall zu verursachen. Die Datenaufsicht erachtete den Einsatz des Senders als Massnahme im Sinne der Einschränkung der Bewegungsfreiheit nach Art. 383 ZGB für zulässig, also als letztes Mittel bei akuter Gefährdung der körperlichen Integrität der Betroffenen oder Dritter unter Einhaltung der Aufklärungspflichten in Art. 383 Abs. 2 ZGB. Dies wurde denn auch so im Merkblatt festgehalten.

Die Datenaufsicht wies zudem darauf hin, dass der Entwurf des Merkblattes für die Bewohnerinnen und Bewohner in Bezug auf die Einwilligungserklärung anzupassen sei. Dieser sah zwei mögliche Erklärungen vor, die »angekreuzt« werden konnten: die Einverständniserklärung, den Rufsender permanent zu tragen oder die Erklärung, den Rufsender nicht permanent tragen zu wollen, unter Inkaufnahme einer möglicherweise entscheidend verzögerten Alarmierung. Nach Ansicht der Datenaufsicht handelte es sich hierbei nicht um eigentliche Einwilligungen, sondern um die Bestätigungen, die möglichen Folgen eines Verzichts an der Teilnahme am Alarmierungssystem zur Kenntnis genommen zu haben. Sie schlug daher vor, die beiden spezifischen Einwilligungsoptionen zu streichen und als Erklärung über die Folgen des Tragens oder Nicht-Tragens des Rufsenders in den Haupttext des Merkblattes einzufügen. Schliesslich müssten die Bewohnerinnen und Bewohner ohnehin das gesamte Merkblatt verstehen, um über den eigenen Umgang mit dem Rufsender entscheiden zu können.

Die Datenaufsicht plant aufgrund der technischen Unzulänglichkeit der Anlage in Bezug auf die Speicherdauer, die Anlage und ihre Nutzung zu einem künftigen Zeitpunkt zu kontrollieren.

2.3 Elektronisches Bewerbungsmanagement

Das Personalamt wandte sich mit der Bitte an die Datenaufsicht, die Umstellung auf ein elektronisches Bewerbungsmanagement zu prüfen. Da die Möglichkeit, das Bewerbungsmanagement elektronisch zu führen grundsätzlich unproblematisch ist, und die benötigte Software als Standardsoftware eingekauft werden konnte, beschloss die Datenaufsicht, die Prüfung auf die organisatorischen und vertraglichen Absicherungen zu beschränken. Dadurch konnte der Prüfungsaufwand gesenkt wer-

den.

Anlässlich einer ersten Besprechung im Oktober 2013 einigten sich die Projektverantwortlichen mit dem Datenschutzbeauftragten auf die rechtlich ausschlaggebenden Punkte für die Ausschreibung der Software. Neben diesen Anforderungen, die insbesondere eine freie Rollendefinition und eine feingliedrige Zugriffssteuerung umfassten, wurden die Notwendigkeit von klar definierten internen Nutzungsabläufen, Bearbeitungsrollen, die Erstellung von Einverständniserklärungen der künftigen Bewerberinnen und Bewerber und die korrespondierende Datenschutzerklärung der Stadt besprochen.

Im Sommer 2014 wurde die Datenaufsicht sodann gebeten, die vertraglichen Bedingungen des Einladungsverfahrens an die Hersteller zu prüfen. Hier zeigte sich, dass die Anwendbarkeit der kantonalen allgemeinen Geschäftsbestimmungen für die Auslagerung von Datenbearbeitungen und Informatikdienstleistungen² mittlerweile bei städtischen Informatikprojekten berücksichtigt und den Anbietern mitgeteilt wird.

Durch die frühzeitige Einbindung der Datenaufsicht konnten die projektspezifischen rechtlichen Anforderungen bereits bei der Einladung zur Offertstellung als Basis für eine künftige Rechtsbeziehung festgelegt werden. Diese beinhalteten neben vertraglichen Pflichten der Parteien Vorgaben an die Anbieter zur Ausgestaltung bzw. Anpassung der Standardsoftware für die spezifischen Bedürfnisse der Stadtverwaltung. Davon profitierten auch die Anbieter, indem der (datenschutz-)rechtliche Rahmen der Offertstellung von Beginn weg klar vorgegeben war.

Nach Vergabe des Projekts prüfte die Datenaufsicht schliesslich die Vereinbarkeit der allgemeinen Geschäftsbedingungen der Anbieterfirma mit den vorgegebenen datenschutzrechtlichen Geschäftsbedingungen sowie dem IDG. Ziel einer solchen Prüfung ist die Herstellung einer gewissen Ausgeglichenheit zwischen den berechtigten Geschäftsinteressen des Anbieters und den gesetzlichen Vorgaben.

3. Öffentlichkeitsarbeit

3.1 Interview zum Thema Datensicherheit an Schulen

Der Datenschutzbeauftragte wurde im Nachgang zur Publikation des Jahresberichts 2014 des kantonalen DSB angefragt, wie es um die Sicherheit der Schulnetze in

² Am 24. Juni 2015 hat der Regierungsrat mit RRB 670 die aktuelle Version der AGB für verbindlich erklärt; abrufbar unter http://www.kitt.zh.ch/internet/finanzdirektion/kitt/de/it_sicherheit.html.

Winterthur bestellt sei.³

Aus Sicht der Datenaufsicht ist die hierfür zuständige SCHU:COM dabei, die Sicherheit der Schulnetze an neue Gegebenheiten anzupassen. Dies betrifft insbesondere die Daten von Schülern, welche die Schularbeit betreffen, etwa Hausaufgaben, die auf dem Schulnetz gespeichert werden oder der Einsatz von Suchmaschinen auf Schulcomputern. Administrative Daten werden dagegen auf dem Stadtnetz geführt, dass von der IDW nach ISO Standard 27001 betrieben wird und mit einer starken 2-Stufen-Authentisierung (SMS und Passwort) gesichert ist.

In diesem Zusammenhang wird in den nächsten Jahren ein Umbau stattfinden, da geplant ist, auf Microsoft Office 365 umzusteigen. Dies ist nun aus datenschutzrechtlicher Sicht grundsätzlich möglich, da die Vertragsbedingungen vonseiten des Herstellers für Bildungseinrichtungen in der Schweiz angepasst wurden. Nun wird die Herausforderung darin bestehen, eine vernünftige Nutzerstrukturierung für diese Onlinedienste festzulegen, damit einerseits die Nutzung durch die Schülerinnen und Schüler möglichst einfach ist, andererseits eine dem Alter, der IT-Kompetenz sowie dem jeweiligen Einsatzgebiet angepasste Sicherheit gewährleistet wird. Während etwa ausgefüllte Mathematikblätter oder Schreibübungen klassenweise gespeichert werden könnten, wird dies in höheren Stufen in Bezug auf Aufsätze möglicherweise nicht mehr vertretbar, aber auch nicht mehr nötig sein, da die Schülerinnen und Schüler mit zunehmendem Alter besser mit eigenen Passwörtern umgehen können.⁴

Ein weiteres Problemfeld wird die Frage eröffnen, inwiefern administrative Daten der Schulen mit Office 365 bearbeitet – und insbesondere auf Servern von Microsoft gespeichert – werden dürfen. Hier stehen noch Abklärungen beim kantonalen Datenschutzbeauftragten aus, deren Ergebnis grundsätzlich darüber entscheiden wird, wie etwa mit medizinischen Daten zu verfahren sei.

4. Internes

4.1 Zusammenarbeit mit anderen Datenschutzbehörden

Der Datenschutzbeauftragte hat auch in diesem Jahr an zwei Tagungen der Vereinigung privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, teil-

³ Anlass war die Schwerpunktsetzung des kantonalen DSB auf das Thema Datensicherheit und Datenschutz an Schulen; der Bericht ist abrufbar unter https://dsb.zh.ch/internet/datenschutzbeauftragter/de/ueber_uns/taetigkeitsberichte.html.

⁴ In diesem Zusammenhang hat der Datenschutzbeauftragte auch schon laut darüber nachgedacht, ob möglicherweise auf eine biometrische Authentisierung gewechselt werden könne. Die betreffenden Systeme werden zunehmend günstiger, weisen indes eigene, spezifische Risiken in Bezug auf die Datensicherheit auf.

genommen. Diese Anlässe dienen dem Austausch mit Kolleginnen und Kollegen aus der ganzen Schweiz und bieten jeweils praxisorientierte Weiterbildungen durch Vortragsreihen und Diskussionsrunden zu Themen, welche für die kantonalen und kommunalen Datenschutzstellen von Interesse sind.

Im Berichtsjahr betrafen die Themen das neue Nachrichtendienstgesetz des Bundes, insbesondere in Bezug auf die Schnittstellen zu den kantonalen Polizeibehörden und Aufsichtsstellen sowie Fragen im Spannungsfeld zwischen Zugang und Schutz von Daten, e-Government und Open Government Data, d.h. die Bereitstellung statistischer Daten zur Nutzung in Apps (mehrheitlich) auf Telefonen und Tablets. Im Hinblick auf die Bestrebungen der Stadt, e-Government-Portale zu schaffen bzw. zu erweitern, sowie auf Fragen in Zusammenhang mit Geoinformations- und anderen statistischen Daten der Stadt, konnte der Datenschutzbeauftragte einige wichtige Hinweise mitnehmen.

5. Ausblick

Nach wie vor ist es dem Datenschutzbeauftragten nicht gelungen, die Zeit zu finden, um eine ordentliche Kontrolle im Sinne eines Datenschutzaudits durchzuführen. Da die Liste der möglichen Kandidaten nach fünf Jahren eine Handvoll Bereiche umfasst, soll nun im Sommer ein neuer Versuch unternommen werden. Allerdings zeigen die ersten Monate des neuen Jahres einen erneuten, deutlichen Anstieg der Fallzahlen, die sich zurzeit auf dem Niveau des bisherigen »Rekordjahres« 2013 bewegen.

Ebenso soll versucht werden, die Fallzahlen weiter zu konsolidieren, eine Schulung für Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung zu organisieren, die von der Datenaufsicht als »Multiplikatoren« für die Sensibilisierung in Datenschutzbelangen identifiziert werden und die Erscheinungsform des Tätigkeitsberichts im Hinblick auf die Wirksamkeit in der Öffentlichkeit zu überarbeiten.

Winterthur, 2. Mai 2016

Datenaufsicht der Stadt Winterthur



Philip Glass, Datenschutzbeauftragter

6. Anhang

6.1 Thematische Übersicht

Im Berichtsjahr eröffnete der Datenschutzbeauftragte auf Anfragen von Behörden und Privatpersonen hin in den folgenden Bereichen neue Dossiers.

- Abstimmungen, Wahlen, statistische Analysen
- Altersresidenzen, Rufanlagen, Perimeteralarmierung
- Anonymisierung von Steuerdaten, Datenabzug zur Softwarepflege, Bekanntgabe an Softwareanbieter, Bekanntgabe von Daten juristischer Personen an Stadtentwicklung
- Beitragsreglement Schulzahnpflege, medizinische Daten
- Content Filter, Ausnahmen Cloud Computing, Zugriff auf Google Formulare, Dropbox, My Drive, BasecampHQ
- Datenbank NEST, Anfragen für Zugriffe
- Datenbearbeitung durch Private in öffentlichem Auftrag
- Datenbekanntgaben zu wissenschaftlichen Zwecken, GIS Wärmedaten, Stromverbrauchsanalysedaten, Wirtschaftsdaten, Geldflussanalysen
- Datensperren, Zuständigkeiten, Einrichtung durch Private
- Dokumentenklassifizierung
- E-Government, Bewerbungsmanagement
- Einsichtsrechte, Polizeijournal, KJZ Winterthur, Spitex, Datensperren, Daten Personalbefragung
- Einwohnerkontrolle, Adresslisten, Bekanntgabe zu ideellen Zwecken, Zugriffsgesuche GREKOS
- Extranet GGR, Zugriffsberechtigungen
- Finanzkontrolle, Einsichtsrechte, Vorgehen bei vermuteten Datenschutzverletzungen
- Glasfasernetz, Kooperation mit privaten Firmen, Vertragsgestaltung, Vermarktung, Betroffenenrechte, Feedbackprozesse
- Grossraumbüros, Vertraulichkeit, Hausordnung, Vernetzung vorhandener Reglemente
- Informationssicherheit, Prozesse, Schutzbedarfs- und Risikoanalysen, Beurteilung von Prozessabläufen, kantonale Verordnung
- Informationssicherheit, technisch und organisatorisch Superblock
- Internes Kontrollsystem IKS
- Kaderschulung
- Lohndaten, Lohnmeldeverfahren
- Mailverteiler Flughafengefängnis
- Melderegistergesetz, Änderungen zum Gemeindegesetz
- Mitarbeiterdaten, Zugriff auf Mails im Krankheitsfall, Ortungsdaten
- Projektmanagementsoftware
- Schulen, elektronisches Absenzenwesen, Profilmanager OSX im Schulnetz, Kryptographie, Datensicherheit, HTTPS-Handling, Office 365

6.2 Bearbeitungsstand der Dossiers per 31. Dezember 2015

Jahr	Eingänge	Erledigungen	Pendent	Total bearbeitet
2012	59	54	21	75
2013	80	65	36	101
2014	68	58	46	104
2015	64	66	44	110

6.3 Aufschlüsselung der Neueingänge nach Aufgaben gemäss § 34 IDG

Aufgabengebiet	Anzahl Dossiers
Beratung der städtischen Behörden	29
Beratung von Privaten	8
Überwachung der Durchführung des Datenschutzrechts, inkl. Vorabkontrollen und Beurteilungen von Bearbeitungsgesuchen	13
Information der Öffentlichkeit über den Datenschutz	1
Angebot Aus- und Weiterbildung in Fragen des Datenschutzes	
- Auf Anfrage einer Behörde	2
Zusammenarbeit mit anderen Datenschutzbehörden	3
Interne Aufgaben (Organisation, Buchhaltung, Jahresbericht, Weiterbildung)	8