Kanton Zürich
Direktion der Justiz und des Innern
Generalsekretariat

Verordnung über die Datenbearbeitung der Direktion der Justiz und des Innern

Entwurf	Erläuterungen
Verordnung über die Datenbearbeitung der Direktion der Justiz und des Innern (vom ...) *Der Regierungsrat,* *gestützt auf § 151 b Abs. 3 und § 151 c Abs. 2 GOG, § 27 c Abs. 3 des Straf- und Justizvollzugsgesetzes vom 19. Juni 2006 (StJVG) und § 9 b Abs. 2 und 3 des Einführungsgesetzes zum Opferhilfegesetz vom 25. Juni 1995 (EG OHG)* *beschliesst:*	
Zweck der Datenbearbeitung	*§ 1. Zweck der Datenbearbeitung*
§ 1. Die Datenbearbeitung in den Verwaltungseinheiten der Direktion der Justiz und des Innern (Direktion) dient folgenden Zwecken:	Die Bestimmung listet die Zwecke der Datenbearbeitung auf. Die Bestimmung bezieht sich auf die Bearbeitung sämtlicher Datenkategorien (gewöhnliche und besondere Personendaten und Sachdaten), beschränkt auf die jeweiligen Datenbearbeitungszwecke der einzelnen Verwaltungseinheiten. Im Bereich der einheitenübergreifende Zugriffe, sind die gesetzlichen Grundlagen in GOG, StJVG und EG OHG massgebend.
a. der Geschäftsverwaltung und Geschäftskontrolle,	lit. a: Die Geschäftsverwaltung (d.h. die Erfassung von Personen- und Geschäftsdaten für die Verwaltung der Geschäfte) soll langfristig zuverlässige, überschaubare und aktuelle Informationen zu Geschäften bereitstellen und diese In-

	formationen für die Nutzerinnen und Nutzer zugänglich machen. Die Geschäftstätigkeit soll in allen Bearbeitungsstadien übersichtlich dokumentiert und die Geschäftsprozesse klar strukturiert sein. Das Verwaltungshandeln wird damit nachvollziehbar und die Rechenschaftsfähigkeit ist gewährleistet. Die Geschäftsverwaltung umfasst also die Registratur des einzelnen Geschäfts, seine Zuteilung an einzelne Mitarbeitende und die Strukturierung des Geschäfts. Teil der Geschäftsverwaltung ist auch die Erfassung der Daten der involvierten Personen. Im Gegensatz zu lit. c (Dokumentenverwaltung) bezieht sich die Geschäftsverwaltung nicht auf die Inhalte einzelner Dokumente in einem Geschäft, sondern auf die Anlage und Verwaltung des Geschäfts mittels Metadaten. Die Datenbearbeitung dient zudem dem Zweck der Steuerung, Planung und Kontrolle der Geschäftsbearbeitung (Controlling), z.B. für die Ermittlung der KEF-Kennzahlen und die Erstellung der Jahresberichte.
b. der Termin- und Fristenkontrolle,	lit. b: Die Speicherung der Daten soll eine effiziente Termin- und Fristenkontrolle durch die Mitarbeitenden der Direktion ermöglichen.
c. der Dokumentenverwaltung,	lit. c: Die Verwaltung der einzelnen im Rahmen eines Geschäfts bearbeiteten Dokumente soll so vorgenommen werden, dass diese den Mitarbeitenden zur weiteren Bearbeitung zur Verfügung stehen. Dazu gehört auch die Dokumentenverwaltung.
d. der Suche von Geschäften und Dokumenten,	lit. d: Das Abfragen von Geschäften, die einen Zusammenhang mit anderen zu bearbeitenden Geschäften aufweisen, muss sichergestellt werden. Zudem muss das Suchen von einzelnen Dokumenten für die Zugriffsberechtigten möglich sein. Vor allem für externe Nutzer ist diese Zugriffsmöglichkeit auszuschliessen (vgl. § 151 Abs. 3 lit. b GOG und 27 a StJVG). Aber auch intern sind Zugriffsbeschränkungen denkbar.
e. der Buchhaltung,	lit. f: Zur Buchhaltung gehört insbesondere die Abrechnung von Verfahrenskosten,

	aber auch die Verwaltung von Klientenkonti im Rahmen des Strafvollzugs.
f. der Evaluation von Geschäftsvorgängen,	lit. h: Die Bewertung von Geschäftsvorgängen ist insbesondere notwendig für die Verbesserung der staatlichen Tätigkeit.
g. dem Wissenserhalt und -austausch,	lit. i: Geschäfte und Dokumente einer Verwaltungseinheit sollen den Mitarbeitenden dieser Einheit – in anonymisierter oder unanonymisierter Form – für die Bearbeitung von anderen, ähnlichen Geschäften zur Verfügung stehen.
h. der statistischen Auswertung und der Forschung.	lit. j: Die Verwaltung und Ablage von Geschäften und Dokumenten soll statistische Auswertungen ermöglichen. Zudem sollen die Daten auch für die Forschung zugänglich gemacht werden können. Beides ist jedoch nur im Rahmen von § 9 Abs. 2 und § 18 IDG und § 21 IDV zulässig (Anonymisierung und keine Rückschlüsse auf betroffene Personen, schriftliches Gesuch bei Bekanntgabe von Daten an Stellen ausserhalb der jeweiligen Verwaltungseinheit oder an Dritte).
Zugriffsrechte innerhalb einer Verwaltungseinheit	*§ 2. Zugriffsrechte innerhalb einer Verwaltungseinheit*
§ 2. [1] Innerhalb einer Verwaltungseinheit haben die Nutzerinnen und Nutzer Zugriff auf die Daten in ihrem Zuständigkeitsbereich.	Der freie Zugang zu den Daten im eigenen Zuständigkeitsbereich muss sichergestellt werden, ist doch ohne diesen Zugang effizientes Arbeiten undenkbar. Das heisst nicht, dass Zugriff auf sämtliche Daten der eigenen Verwaltungseinheit besteht (z.B. beim Generalsekretariat auf sämtliche Daten die von den Mitarbeitenden bearbeitet werden). Vielmehr gibt es Bereiche, die einem gewissen Kreis von Mitarbeitenden vorbehalten sein müssen. Der Zugriff besteht einerseits elektronisch. Die Bestimmung umfasst aber auch den physischen Zugriff auf Papierakten. Die Bestimmung gilt damit für Papierakten und elektronisch gespeicherte Daten gleichermassen.
[2] Jede Verwaltungseinheit legt die Zugriffsrechte für die einzelnen Funktionen fest.	Für jede Verwaltungseinheit muss deren Leitung ein Zugriffskonzept erlassen und

Sie informiert die Direktion darüber.	die Zugriffsrechte der Mitarbeitenden den Funktionen entsprechend zuteilen. Dies kann in einer Matrix erfolgen, analog zu derjenigen zu den Zugriffsberechtigungen zur Lotus-Notes-Datenbank des Regierungsrates (vgl. RRB Nr. 1346/2010). Es erscheint nicht als sinnvoll, die Zugriffskonzepte in einen Verordnungsanhang aufzunehmen, müsste doch der Regierungsrat dann bei jeder Änderung erneut entscheiden. Zudem würde den Verwaltungseinheiten die nötige Flexibilität genommen. Zu Kontrollzwecken sind die Zugriffsberechtigungen der Direktion mitzuteilen.
Zugriffsrechte von Nutzerinnen und Nutzern anderer Verwaltungseinheiten	*§ 3. Zugriffsrechte von Nutzerinnen und Nutzern anderer Verwaltungseinheiten*
§ 3. [1] Der elektronische Zugriff von Nutzerinnen und Nutzern anderer Verwaltungseinheiten der Direktion und der Polizeien gemäss § 151 a Abs. 1 lit. b und c GOG, § 27 b lit. a StJVG und § 9 a EG OHG ist auf Daten beschränkt, die der Geschäftsverwaltung dienen.	Der Zugriff von Nutzerinnen und Nutzern anderer Verwaltungseinheiten der Direktion und der Polizeien muss sich gemäss § 151 b Abs. 3 GOG auf Geschäftsverwaltungsdaten (Metadaten) – das sind Angaben zu Personen, die an den behandelten Geschäften beteiligt sind (Personendaten), sowie auf grundlegende Informationen zu den bearbeiteten Geschäften (Gegenstand des Geschäfts, Erledigungsart und Erledigungsdatum u.ä.) – beschränken, dabei handelt es sich um Findmittel gemäss § 151 b Abs. 3 GOG. Diese Regelung schliesst einen Zugriff von externen Nutzerinnen und Nutzern auf einzelne Dokumente aus, so insbesondere auf Urteile oder Gutachten in Strafverfahren. Der Zugriff auf Geschäftsverwaltungsdaten ermöglicht die Beurteilung, ob zusätzliche Akteneinsicht notwendig ist. Wird dies als notwendig erachtet, müssen die Akten im Einzelfall beigezogen werden. Diese Gesuche sind nach dem massgebenden Verfahrensrecht (StPO, JStPO, VRG) oder dem IDG zu beurteilen.
[2] Die Oberstaatsanwaltschaft, die Oberjugendanwaltschaft und die Leitung des Amtes für Justizvollzug entscheiden über die Erteilung des Zugriffsrechts für Nut-	Diejenige Verwaltungseinheit, welche die Datenhoheit hat, entscheidet darüber welchen (und insbesondere wie vielen) externen Nutzerinnen und Nutzern die

zerinnen und Nutzer anderer Verwaltungseinheiten der Direktion und der Polizeien und stellen die Beschränkung des elektronischen Zugriffs sicher.	Zugriffsberechtigung zu erteilen ist. Massgebend sind die Regeln und Voraussetzungen der Amtshilfe. Sie vergibt auch die dazu notwendigen Berechtigungen. Diese Verwaltungseinheiten sind auch verpflichtet sicherzustellen, dass der Zugriff auf die Daten der Geschäftsverwaltung beschränkt ist.
[3] Sie informieren die Direktion über die gewährten Zugriffsberechtigungen.	Die Erteilung von Zugriffsberechtigungen ist der Direktion mitzuteilen.
Zugangssicherung	*§ 4. Zugangssicherung*
§ 4. Die Nutzerinnen und Nutzer erhalten nach der erfolgreichen Prüfung ihrer Identität Zugang zu den elektronischen Daten.	Die Identität der Person, die elektronische Daten bearbeiten will, muss mittels eines „Log-in“ erfragt werden. Nur bei erfolgreicher Prüfung der Identität (Authentifizierung) wird die Kommunikationsbeziehung fortgesetzt. Der Vorgang soll nicht auf Chip-Karten beschränkt werden, da auch andere Prüfsysteme denkbar sind (Iris-Scanner; Fingerabdruck u.ä.).
Protokollierung	*§ 5. Protokollierung*
§ 5. [1] Der elektronische Zugriff auf Daten wird protokolliert. Die für die Datensicherheit verantwortliche Person der Direktion und ihre Stellvertretung haben Zugriff auf die Protokolle.	Durch die Protokollierung der Zugriffe können diese kontrolliert werden. Die Gefahr von Missbrauch kann so eingeschränkt, bzw. Missbrauch festgestellt werden. Die für die Datensicherheit zuständige Person wird im Rahmen der Organisationsverordnung der Direktion der Justiz und des Innern (JIOV) zu bezeichnen sein.
[2] Die Protokolle werden ein Jahr aufbewahrt und anschliessend automatisch gelöscht.	Eine Aufbewahrungsfrist von einem Jahr erscheint als ausreichend. Nach Ablauf dieses Jahres sind die Protokolle automatisiert zu löschen.

Eingeschränkter Datenzugriff	*§ 6. Eingeschränkter Datenzugriff*
§ 6. [1] Der Zugriff auf Daten, die aufgrund einer spezialgesetzlichen Regelung länger als zehn Jahre aufbewahrt werden, ist den Nutzerinnen und Nutzern der betreffenden Verwaltungseinheit vorbehalten.	Werden Akten gestützt auf die spezialgesetzlichen Vorschriften (Art. 103 StPO, § 151 c GOG, § 27 a GOG) länger als zehn Jahre aufbewahrt, soll der Zugang zu ihnen eingeschränkt werden. Dies gilt sowohl für Papierakten als auch für elektronische Akten. Verfahrensakten, die über die ordentliche Frist hinaus aufbewahrt werden, werden dadurch dem allgemeinen Zugriff entzogen.
[2] Die Leiterin oder der Leiter der Verwaltungseinheit beschränkt die elektronische Zugriffsberechtigung auf einzelne Mitarbeitende.	Ein elektronischer Zugriff auf diese Daten soll nur einem eingeschränkten Kreis von Mitarbeitenden der entsprechenden Verwaltungseinheit möglich sein. Zusätzlich soll der Zugriff von der Leiterin oder dem Leiter der Verwaltungseinheit noch zusätzlich auf einen engen Kreis von Mitarbeitenden beschränkt werden. Denkbar ist insbesondere, dass eine Anfrage bei einer zentralen Stelle gestellt werden muss.