Kanton Zürich
Direktion der Justiz und des Innern
Generalsekretariat

Datenschutz und Informationssicherheit in der Direktion der Justiz und des Innern

Bericht und Aktionsplan

Zürich

19.12.2023

Fassung vom:	19. Dezember 2023
Version:	1.1 (ohne Personendaten)
Status:	Final

Vorwort der Direktionsvorsteherin

Staatliche Institutionen haben in ihrem Umgang mit Datenschutz und Informationssicherheit eine Vorbildrolle. Das betrifft den Kanton Zürich als Ganzes und ebenso die Direktion der Justiz und des Innern (JI), welche aufgrund ihrer Zuständigkeiten als «Datendirektion» gilt.

Mit dieser Vorbildrolle ist eine Verantwortung verbunden. Diese Verantwortung wollen wir mit dem vorliegenden Bericht wahrnehmen.

Mit dem Auf- und Ausbau der digitalen Kommunikation sind die Anforderungen an den Datenschutz und die Informationssicherheit sowie an das Datenmanagement und den Umgang mit Daten gestiegen. Nun geht es darum, die Strukturen, das Bewusstsein und das Knowhow auf kantonaler Ebene – innerhalb der Direktionen sowie in den einzelnen Organisationseinheiten – den Anforderungen anzupassen. Die JI ist bestrebt, hier Pionierarbeit zu leisten. Dabei haben wir den Anspruch, dass die gesamte kantonale Verwaltung von dieser Arbeit profitieren soll. Der Bericht zeigt auf, wo unsere Bemühungen schon Früchte tragen und wo noch Handlungsbedarf besteht.

In der JI ist es zu einem Datenvorfall gekommen, der zwar bereits rund 15 Jahre zurückliegt, der aber gleichwohl eine gründliche Analyse der Organisation verlangt. Nur so lässt sich sicherstellen, dass wir aus den gemachten Erfahrungen die richtigen Schlüsse gezogen haben.

Konkret wurde überprüft, ob und wie die Empfehlungen der Administrativuntersuchung umgesetzt sind, die ich Ende 2020 in Auftrag gegeben hatte. Da sich diese Untersuchung auf die vom Datenvorfall direkt betroffenen Organisationseinheiten beschränkt hatte, soll der vorliegende Bericht aber einen Schritt weiter gehen und sich auch dazu äussern, wo die Direktion insgesamt punkto Datenschutz und Informationssicherheit steht.

Das Thema Datenschutz und Informationssicherheit ist insbesondere in den Einheiten mit besonders sensiblen Daten wie der Strafverfolgung, dem Strafvollzug oder dem Staatsarchiv bereits organisatorisch abgebildet. Die direktionsweite Etablierung gelingt darüber hinaus nur, wenn alle Mitarbeitenden davon überzeugt und motiviert sind, sich auf diesem Weg weiterzuentwickeln. Voraussetzung für eine solche Haltung der Mitarbeitenden ist eine offene Fehlerkultur. Diese möchten wir mit dem Bericht unterstreichen. Unsere Botschaft ist: Gemeinsam wollen wir uns in diesem zentralen Thema vorwärtsbewegen. Gemeinsam wollen wir verändern.

Wir werden Erfolg haben, wenn wir neben der Fehlerkultur auch unser Knowhow und unsere Prozesse stärken. Es braucht ein solides Wissen bei den Mitarbeitenden. Und es braucht klare, einfache Vorgaben und Prozesse. Auf dieser Basis können die Mitarbeitenden die neuen Möglichkeiten in der Kommunikation und der Zusammenarbeit nutzen und gleichzeitig dem Datenschutz und der Informationssicherheit gerecht werden.

Inhaltsverzeichnis

Einleitung

Die Umsetzung des Datenschutzes und der Informationssicherheit (im Folgenden «D&I») stellt die kantonale Verwaltung vor besondere Herausforderungen.

Den rechtlichen Rahmen bildet das kantonale Gesetz über Information und Datenschutz mit dessen Ausführungsbestimmungen (IDG / IDV / IVSV). Aktuell befinden sich diese Rechtsgrundlagen in Revision. Hierauf soll bei der Umsetzung der Massnahmen Rücksicht genommen werden. Weiter sind – anders als im privatwirtschaftlichen Sektor – das Öffentlichkeitsprinzip sowie das Legalitätsprinzip zu berücksichtigen, was höhere Anforderungen an die Prozessdefinitionen, die Regelungsdichte sowie die Kommunikation stellt. Schliesslich gilt es in verschiedenen Bereichen, namentlich der Strafverfolgung und dem Justizvollzug, Spezialvorschriften zu beachten. Dasselbe gilt für die Archivierung: Anders als die Privatwirtschaft, müssen öffentliche Organe die wichtigsten Informationen, die sie produzieren, nicht nur für eine bestimmte Zeit aufbewahren, sondern in originaler Form dauernd überliefern.

Im Rahmen dieses Projektes konnte die JI von der Erfahrung der KPMG bei der Umsetzung des neu revidierten eidgenössischen Datenschutzgesetzes (DSG) sowie dessen Implementierung im privaten Sektor sowie beim Bund profitieren. Zugleich sind die oben erwähnten Unterschiede und Besonderheiten zu Tage getreten. Hierzu wird bei den einzelnen Empfehlungen eingegangen.

Die kantonale Verwaltung ist eine überaus komplexe, heterogene und dezentral strukturierte Organisation. Dies trifft auch für die JI selbst zu: Sie umfasst Organisationseinheiten von den Fachstellen mit wenigen Mitarbeitenden bis zum Amt Justizvollzug und Wiedereingliederung (JuWe) mit mehr als 1000 Mitarbeitenden. Die Organisationseinheiten weisen nicht nur unterschiedliche Grössen aus, sondern haben ihre Aufgaben in äusserst unterschiedlichen Fachbereichen und auch der Charakter der Tätigkeiten unterscheidet sich stark: von der Strafverfolgung über den Justizvollzug mit Vollzugsinstitutionen bis zur Kulturförderung.

Die Querschnittfunktionen, wozu die Informations- und Kommunikationstechnologie zu zählen ist, werden sowohl auf kantonaler wie auch auf direktionaler Ebene gesteuert. Insbesondere die kantonale Ebene, namentlich das Amt für Informatik, die «Strategischen Initiativen» bei der Staatskanzlei etc. wurden neu geschaffen und es ist damit umzugehen, dass innerhalb der JI auch die Ämter im Bereich IKT sehr unterschiedlich organisiert sind (vgl. IKT-Strategie des Kantons Zürich, RRB Nr. 383/2018). Dies gilt es bei der Ausgestaltung der Zuständigkeiten und der wirkungsvollen Allokation der Aufgaben im Bereich D&I zu berücksichtigen. So sollten gewisse Regeln sinnvollerweise auf kantonaler Ebene erlassen werden, vgl. hierzu unsere Stellungnahmen zu den einzelnen Themen.

Hybrides Arbeiten: Innerhalb der JI bestehen nach wie vor wichtige Bereiche (Strafverfolgung, Justizvollzug), in denen das massgebende Dossier analog geführt wird und zusätzlich digitale Informationen zum Geschäft bestehen. Die Verwaltung wird noch längere Zeit sowohl mit analogen wie auch mit elektronisch gespeicherten Daten umzugehen haben. Bei den Regelungen und Sicherheitsmassnahmen sowie der Schulung der Mitarbeitenden gilt es dies zu berücksichtigen, z.B. bei der Einführung einer «Clean desk policy». Dies stellt eine besondere Herausforderung dar und sollte sich mit dem Voranschreiten der digitalen Transformation verbessern.

Die JI widmet dem Datenschutz und der Informationssicherheit (D&I) grosse Aufmerksamkeit, insbesondere mit Blick auf die digitale Transformation. So interpretieren wir das Resultat der Erhebung der KPMG. Die Durchführung der Erhebung mittels Umfrage und 35 vertiefenden Interviews hat das Bewusstsein in den Organisationseinheiten für das Thema D&I weiter geschärft. Zudem wurde Wert darauf gelegt, allfällige Erkenntnisse zu Verbesserungsmöglichkeiten aus der Umfrage noch während des laufenden Projektes direkt

umzusetzen. Die Einführung des DAP sowie des Digilex (elektron. Verfahrensführung) bieten aktuell ebenfalls Möglichkeiten, viele Mitarbeitende zum Thema D&I zu erreichen.
Angesichts der Bedeutung für die Organisation wurde das Drittparteienmanagement bzw. die Auftragsdatenbearbeitung in einem gesonderten Projekt geführt (vgl. Ziff. 3.8) und vorgezogen, weshalb es hier nur am Rande behandelt wird. Dieses Projekt konnte zwischenzeitlich abgeschlossen und die Organisationseinheiten hierzu informiert werden

1 Erhebung durch die KPMG

1.1 Ausgangslage

Dem effektiven Datenschutz sowie der hohen Informationssicherheit kommt beim Kanton Zürich und insbesondere bei dessen Direktion der Justiz und des Innern [JI], welche mit besonders sensiblen Informationen arbeitet, besonderes Gewicht zu.

Entsprechend gibt es in der JI zu D&I viele Grundlagen. Die meisten Verfahren im Austausch mit Bürgerinnen und Bürger sind in der JI aufgrund der derzeitigen Rechtsgrundlagen noch analog ausgestaltet (z.B. im Bereich Strafverfolgung, formelles erstinstanzliches Verwaltungsverfahren, Rekursverfahren). Der Fokus der D&I -Grundlagen in der JI zielt damit ebenfalls noch relativ stark auf die physischen Dokumente ab. Die bestehenden D&I-Massnahmen zeigten denn auch im physischen Dokumentenbereich höhere Wirksamkeit als im elektronischen Informationsbereich.

Es sei in diesem Kontext hier angemerkt, dass im elektronischen Informationsbereich, welcher nicht im Fokus dieser Befragung lag, zur Zeit diverse Neuerungen anstehen, welche den D&I substanziell zu verbessern in der Lage sind. Damit werden die heutigen Schutzmassnahmen wie z. B. die bereits eingeführte bzw. sich flächendeckend auf dem Weg befindliche Einführung der sog. Two Factor Authentication, wo zusätzlich zur Autorisierung mittels Passwort Chipkarten oder Fingerprints eingesetzt werden, weiter verbessert.

1.2 Zielsetzung

Die JI setzte sich mit Blick auf die rasch voranschreitende Digitalisierung das **Ziel, den gegenwärtigen Stand des Datenschutzes und der Informationssicherheit in den einzelnen Organisationseinheiten der JI zu erheben und für die ganze JI ein möglichst einheitliches D&I-Regelwerk zu etablieren**. Dieses soll von allen Mitarbeitenden verstanden, mitgetragen und gelebt werden.

Um dieses Ziel zu erreichen, wurde zwischen dem 11. Mai und dem 24. Juli 2023 in den Organisationseinheiten der JI eine Erhebung **«Datenschutz und Informationssicherheit in der JI» [D&I@JI] durchgeführt**. Die technische Informationssicherheit war dabei nicht Gegenstand der Erhebung. Diese wird zentral vom Amt für Informatik bzw. der Digital Solutions der JI (DigiSol) verantwortet.

Der vorliegende Bericht soll die weiteren Arbeiten im Bereich D&I strukturieren und priorisieren. Als wichtiges Resultat des Berichts soll aufgezeigt werden, welche Massnahmen und Ressourcen nötig sind, um die heutigen Vorgaben im Bereich D&I hinlänglich zu erfüllen. Der Bericht soll zudem aufzeigen, auf welcher Stufe (Kanton, Direktion oder Amt) die einzelnen Arbeiten sinnvollerweise angegangen werden sollen.

1.3 Vorgehen

Das Vorgehen erfolgte in vier Schritten:

1. Umfrage zum Stand des Datenschutzes und der Informationssicherheit in der JI: Mittels einer Umfrage wurde der Stand des D&I in den einzelnen Organisationseinheiten der JI erhoben An der Umfrage nahmen in der Regel eine Person je Organisationseinheit teil.
2. Vertiefungsinterviews: Hernach wurden vertiefende Interviews mit den bereits an der Umfrage teilgenommenen Personen durchgeführt. Damit konnten die in der Umfrage erhobenen Informationen geschärft und – je nach Wissensstand der befragten Personen – ergänzt oder korrigiert werden. Dadurch konnte ein klareres, ganzheitlicheres Bild generiert werden.
3. Feststellungen: Aus den Interviews wurden die wesentlichen Feststellungen pro untersuchtem Handlungsfeld zusammengetragen. Zudem wurde eine Bewertung der im Rahmen der Analyse identifizierten Risiken mit Blick auf das zurzeit rechtskräftige IDG im Sinne einer Risikoeinschätzung vorgenommen.
4. Handlungsempfehlungen: Basierend auf den Feststellungen wurden Handlungsempfehlungen ausformuliert und priorisiert.

Auftragsgemäss basieren die Erkenntnisse auf den Aussagen und dem Wissensstand der befragten Personen. Dies hatte zur Folge, dass insbesondere die Vertreterinnen und Vertreter der kleineren Organisationseinheiten bzw. ohne fachlichen Hintergrund zu D&I zu einigen Fragen keine oder auch nicht ganz akkurate Auskunft geben konnten. Dies gilt es bei der Interpretation der Resultate zu berücksichtigen und wird in der Stellungnahme der JI zu den einzelnen Empfehlungen adressiert, soweit es nicht vorgängig aufgefangen werden konnte.

Weiter wurde die Befragung ausschliesslich innerhalb der JI durchgeführt. Die entsprechenden Organisationseinheiten auf kantonaler Ebene, wie namentlich das AFI, wurden in die Erhebung nicht miteinbezogen.

Zusammenfassend kann festgehalten werden: Während den Interviews zeigte sich ein durchgehend gutes Grundverständnis für die Erfordernisse des Amtsgeheimnisses und die Sensibilität der bearbeiteten Informationen. Die interviewten Personen waren entsprechend besorgt und motiviert, dass D&I hochgehalten werden und haben erkannte Probleme und ungeklärte Fragen offen angesprochen. Dies war der Qualität der Befragung äusserst zuträglich. Wir fanden damit in der JI nicht nur eine konstruktive Fehlerkultur vor, sondern auch eine sehr hohe Motivation, Lücken rasch zu schliessen und den Umgang vor allem mit elektronischen Informationen zu verbessern. Letzteres hat auch dazu beigetragen, dass sehr konkrete, am richtigen Ort ansetzende und damit effektive Handlungsempfehlungen ausformuliert werden konnten.

Angesichts von Anzahl und Umfang der Handlungsempfehlungen sowie der sehr vielen, begonnenen Arbeiten ist bereits an dieser Stelle festzuhalten, dass es mit den im JI gegenwärtig vorhandenen Ressourcen nicht möglich sein wird, D&I auch zukünftig im mindestens erforderlichen Umfang sicherzustellen, um den heutigen, rasch wachsenden Risiken und kommenden gesetzlichen Anforderungen gerecht zu werden (vgl. hinten Kapitel 4.3 und 4.4).

1.4 Haupterkenntnisse

Aus der Umfrage und den Interviews ergaben sich die folgenden Haupterkenntnisse:

a. **Verantwortlichkeiten**: Für den Bereich D&I gibt es bereits zahlreiche Regelungen auf Gesetzes- und Verordnungsstufe (insb. IDG, IDV, IVSV, Organisations- und Verfahrenserlasse), welche zum Teil weiter konkretisiert werden in Richtlinien (z.B. Allgemeine Informationsrichtlinien, Besondere Informationsrichtlinien, Handbuch IKT Governance, Informationssicherheits-Kontroll-Framework) oder in Organisationsreglementen auf Stufe Organisationseinheit. Die damit verbundenen Aufgaben und Verantwortlichkeiten und die operationelle Durchführung von Kontrollen in den Organisationseinheiten müssen jedoch präziser definiert und klarer einzelnen Stellen und Personen zugewiesen werden.

b. **Verzeichnisse über die Informationsbestände:** Verzeichnisse über die Informationsbestände gemäss § 14 Abs. 4 IDG sind weitgehend vorhanden. Diese sind nicht immer aktuell gehalten, entsprechen im Übrigen aber der heutigen Praxis der öffentlichen Organe im Kanton Zürich und den Anforderungen gemäss IDG und IDV. Um einen besseren Gesamtüberblick über die in der JI bearbeiteten Daten zu erhalten, ist ein direktionsweites und detaillierteres Verzeichnis jedoch erstrebenswert.

c. **Privacy by Design & Default:** Die im europäischen Rechtsraum etablierten Grundsätze «Privacy by Design» (Datenschutz durch entsprechende Technikgestaltung) und «Privacy by Default» (Datenschutz durch datenschutzfreundliche Voreinstellungen) werden wohl erst mit dem totalrevidierten Gesetz über die Information und den Datenschutz (nIDG) explizit und verbindlich eingeführt. Entsprechend fehlt zum heutigen Zeitpunkt ein Rahmenwerk, das die bereits heute bestehenden Elemente – wie z.B. die für den Datenschutz relevanten Projektschritte gemäss der HERMES-Projektmanagementmethode – zusammenführt. Da Privacy by Design & Default Ausfluss des allgemeinen Grundsatzes der Verhältnismässigkeit sind, ist diese bereits heute sinnvollerweise bei datenschutzrelevanten Projekten und IT-Änderungen zu beachten.

d. **Datenschutz-Policy:** Eine einheitliche, für die ganze JI gültige interne Datenschutz-Policy gibt es derzeit nicht. Die aktuellen Datenschutz-Policies orientieren sich an den stark unterschiedlichen Bedürfnissen und Anforderungen der Einheiten in Bezug auf ihre Risikoexponiertheit. Dort, wo besondere Personendaten in grossen Mengen bearbeitet werden (DigiSol, Staatsarchiv, Staatsanwaltschaften, etc.) ist das Bewusstsein für Datenschutzfragen hoch. Deren hohes Niveau soll bei der Vereinheitlichung der Orientierungspunkt sein.

e. **Legitimierungsgrundlagen:** Das geltende IDG kennt die Einwilligung als Rechtfertigungsgrund für die Bearbeitung von Personendaten nicht explizit, sondern nur für den Spezialfall der Datenbekanntgabe. In den wenigen Fällen, in denen heute Einwilligungen in Datenbearbeitungen von den betroffenen Personen eingeholt werden, ist deshalb genauer zu prüfen, ob die Datenbearbeitung gerechtfertigt ist.

f. **Datenmanagement:** Die Sicherstellung von Datenqualität, Aufbewahrung und Löschung/Vernichtung ist im Kanton Zürich noch nicht einheitlich geregelt. Diese Fragen sind Gegenstand eines Projekts der neu gestarteten, kantonsweiten strategischen Initiativen Daten und Organisation. Mit dem Projekt werden die gegenwärtigen Prozesse im ganzen Kanton formalisiert und in eine Datenarchitektur integriert. Bis dahin sind die einzelnen Einheiten für passende Lösungen verantwortlich.

g. **Drittparteienmanagement:** Verträge zu Drittparteien sind in der JI in unterschiedlicher Qualität vorhanden. Während es beispielweise bei der Kantonalen Opferhilfestelle und anderen Stellen einen vorbildlichen Lifecycle-Prozess auch mit Drittanbietern gibt, sind solche integrierte Modelle in verschiedenen Einheiten erst bruchstückhaft vorhanden. Gleiches gilt für die D&I-Audits der Drittparteien.

h. **Informationssicherheit:** Sicherheitsmassnahmen wie etwa Berechtigungskonzepte oder Verschlüsselung bei Datentransfers sind in vielen Fällen vorhanden. Die noch vorhandenen Lücken müssen geschlossen werden. Mit Bezug auf die Klassifikation und Verschlüsselung von Informationen wird in der JI mit dem Rollout des Digitalen Arbeitsplatzes voraussichtlich die Sicherheitslösung «Microsoft Purview» eingeführt.

i. **Schulungen und Sensibilisierungsmassnahmen:** Diese gehören in verschiedenen Einheiten zum Standard. In anderen fehlen sie noch.

j. **Prozess bei Verletzungen der Datensicherheit:** Für den Fall einer Datensicherheitsverletzung gelten der bestehende Standardprozess zur verwaltungsinternen Meldung sowie zur Meldung des Vorfalls an die kantonale Datenschutzbeauftragte (DSB). Die Prozesse sind in vielen Einheiten bekannt. Entsprechend werden auch Meldungen gemacht. Innerhalb der JI gibt es jedoch keine einheitlichen Regelungen betreffend die Zuständigkeit für die Meldung und den Einbezug der Vorgesetzten.

Die folgenden Seiten zeigen eine **Übersicht der Schlüsselempfehlungen der KPMG, aufgeteilt in «Quick Wins» und längerfristige Massnahmen**. Aufgrund der derzeit stattfindenden IDG-Revision empfehlen wir der JI, sich bei der Umsetzung soweit möglich und sinnvoll an dem bereits bekannten revidierten Gesetzesentwurf des IDG (E-IDG) auszurichten.

Für die Sicherstellung der Informationssicherheit sind gemäss IDG dem jeweiligen Risiko angemessene technische und organisatorische Massnahmen zu treffen. Ein effektiver D&I kann hierbei aber nicht mit vertretbaren Mitteln in buchstabengetreuer Weise und per sofort umgesetzt werden. Daraus folgt, dass in der JI wie auch in den übergeordneten Gremien zwangsläufig ein risikobasierter Ansatz gefahren werden muss. Die nach einer sorgfältigen Beurteilung in Kauf genommenen Risiken müssen dokumentiert und einem verantwortlichen D&I Gremium zum Entscheid vorgelegt werden können. Fehlen solche Entscheidungsgremien oder sind sie nicht willens, Risiken zu akzeptieren, bleiben als Konsequenz hiervon die Umsetzungsmassnahmen lange und meist in sehr kostspieliger Weise stecken oder werden gar verunmöglicht. Entsprechend kommt einer funktionierenden, sachkundigen D&I Governance, welche Risiken zu tragen gewillt ist, für eine erfolgreiche Umsetzung der Massnahmen entscheidendes Gewicht zu.

Dieser risikobasierte Ansatz bedingt, dass auch der aktuelle **«State of the Art» in der Umsetzung der D&I-Vorgaben in vergleichbaren Organisationen auch ausserhalb des Kanton Zürich** (betreffend Risiken, Struktur und Grösse; z.B. Bund oder wo vergleichbar Unternehmungen) berücksichtigt werden. Dabei sind jedoch die Besonderheiten der Verwaltung zu beachten (vgl. oben unter 1. Einleitung).

Um die empfohlenen Massnahmen umsetzen zu können, sind folgende Voraussetzungen nötig:

a.) eine hoch in der Verwaltungshierarchie stehende, fachkundige Governance mit Entscheidungskompetenz in Sachen D&I;
b.) ein priorisierter Umsetzungsplan;
c.) die Bereitstellung der für die Umsetzung erforderlichen Mittel;
d.) in der gesamten JI für das Vorhaben hinlängliche, zusätzliche Personalressourcen und Stellenprozente, in der ersten Phase für das Umsetzungsprojekt und hernach für den operativen Betrieb.

In welchem Umfang diese Voraussetzungen erfüllt werden müssen, hängt von der Ausgestaltung der Massnahmen, der Organisation, der Zuständigkeiten, den technischen Möglichkeiten und rechtlichen Rahmenbedingungen ab. In jedem Falle aber muss festgehalten werden, dass es sich hierbei um **ein kostspieliges, langjähriges Grossprojekt mit hohem Veränderungsgrad hinsichtlich organisatorischer und technischer Verfahren handelt**, welches alle Einheiten und Personen innerhalb als auch ausserhalb der JI miteinbezieht. Das Vorhaben darf also bezüglich dessen Dimension keinesfalls unterschätzt werden.

2 Befragungsergebnisse und Handlungsempfehlungen

2.1 Verantwortlichkeit & Organisation

Feststellungen	**Verantwortlichkeit & Organisation:** In den Bereichen der Strafverfolgung und des Justizvollzugs verpflichten § 88b GOG und § 18 a StJVG als Spezialgesetze bereits seit 2020 zur Bestimmung von Personen, die für die Datenschutzberatung ihrer Organisationseinheiten (OE) zuständig sind. Eine solche Funktion sieht der Gesetzesentwurf zum Organisationsgesetz des Regierungsrates und der kantonalen Verwaltung (OG RR) im Rahmen des zu revidierenden IDG nun auch für jede Direktion auf Direktionsstufe vor (§ 44 c E-OG RR). Mit der Anpassung der JIOV auf den 1. Juli 2023 hat sich die JI die Pflicht zur Ernennung von verantwortlichen Personen für den Datenschutz und die Informationssicherheit (sog. D&I-Verantwortliche) auferlegt. So wurden per Juli 2023 in allen OE der JI D&I-Verantwortliche für den D&I ernannt. Das entsprechende Fachwissen in den Bereichen D&I ist nicht in allen OE gleich hoch, was einerseits mit der unterschiedlichen Grösse der einzelnen OE zu tun hat, andererseits mit dem Umstand, dass das D&I-spezifische Risiko sehr unterschiedlich ausgeprägt ist. So

	bestehen z.B. in der Fachstelle Kultur (FK) oder der Fachstelle Integration (FI) geringere Risiken einer Datenschutzverletzung, da diese mit wenigen und wenig sensiblen Personendaten arbeiten. **Verzeichnis der Informationsbestände:** Öffentlich zugängliche Verzeichnisse der Informationsbestände, wie vom IDG gefordert, bestehen mit Ausnahme der FK bei allen Organisationseinheiten. Diese sind nicht immer aktuell gehalten, entsprechen im Übrigen aber der heutigen Praxis der öffentlichen Organe im Kanton Zürich und den Anforderungen gemäss IDG und IDV (insb. Kennzeichnung der Zwecke und Personendaten). Der Aktualisierungsrhythmus ist nicht in allen Einheiten geklärt.
Empfehlungen	Betreffend **Verantwortlichkeit und Organisation** ist auf Ebene Direktion darauf zu achten, dass die D&I-Verantwortlichen, welche gemäss JIOV benannt werden müssen, über die entsprechenden **Fachkenntnisse** (z.B. Weiterbildung im Bereich Datenschutz / Informationssicherheit), **zeitliche und personelle Ressourcen** und **Zugang zur Amtsleitung** verfügen, um insbesondere bei Vorfällen in Zusammenhang mit einer Datensicherheitsverletzung rechtzeitig und angemessen agieren zu können. Weiter empfehlen wir die Definition eines **Pflichtenhefts für die D&I-Verantwortlichen, inkl. Aufgabenprofil, Kompetenzen und Verantwortlichkeiten**. Ebenso zentral ist die **Bewusstseinsbildung** bei den Führungspersonen, damit diese die von den Verantwortlichen angeordneten Massnahmen auch mittragen und in der Lage sind, risikobasierte Entscheide zu treffen. Zur Umsetzung des sich in Revision befindenden IDG ermutigen wir die JI, ein neues **Datenschutz-Risk-&-Compliance-Rahmenwerk** zu definieren. Wir empfehlen bei der Zuteilung der operativen Aufgaben und Verantwortlichkeiten, die betroffenen Bereiche und **Mitarbeitenden** von Beginn an **einzubinden** und am Aufbau des neuen Datenschutz-Rahmenwerks zu beteiligen, damit dieses von Anfang an mitgetragen wird. Für einen besseren Überblick über die Datenbestände und damit ein besseres Controlling in der Direktion empfiehlt sich zudem, ein detaillierteres, direktionsweites Verzeichnis der Informationsbestände zu führen. Ein solches Verzeichnis erübrigt sich gegebenenfalls mit der Einführung eines kantonalen Datenkatalogs gemäss § 44 a E-OG RR. *Empfohlene Umsetzungsebene: Direktion und Organisationseinheit* Zudem verlangt das IDG gemäss § 14 Abs. 4 IDG die Erstellung und Veröffentlichung (und – wo nicht aktuell gehalten – Überarbeitung) der **Verzeichnisse über die Informationsbestände**. Ausser einer kleinen Fachstelle haben alle OE ein solches Verzeichnis veröffentlicht. Für eine bessere Übersicht und ein einfacheres Monitoring empfehlen wir der JI via Generalsekretariat eine Vorlage zu erstellen mit den geforderten Informationen (Zwecke, Personendatenbezug) und diese den Organisationseinheiten zugänglich zu machen. Ein über die Anforderungen des IDG hinausgehendes detaillierteres,

	direktionsweites Verzeichnis der Informationsbestände würde schliesslich der JI einen besseren Überblick über ihre Datenbestände verschaffen und deren Management substanziell erleichtern. Ein solches Verzeichnis müsste sinnvollerweise technisch unterstützt aufgebaut und aktuell gehalten werden. *Empfohlene Umsetzungsebene: Direktion und Organisationseinheit*
Stellungnahme & Massnahmen der JI	**Verantwortlichkeit & Organisation:** Mit Inkrafttreten der totalrevidierten JIOV per 1. Juli 2023 wurden **in allen OE D&I-Verantwortliche** bestimmt. Diese sind für die Umsetzung der D&I-Vorgaben in ihren jeweiligen OEs zuständig und sind erste Ansprechpersonen zu Fragen rund um D&I innerhalb der OE und für das GS JI. Die D&I-Verantwortlichen sollen unter der Leitung des neu geschaffenen **Fachbereichs Informationen und Datenschutz (FB InfoDat)** im GS SRD, zusammen mit dem Informationssicherheitsbeauftragten der JI (ISID), eine Community of Practice (CoP) bilden. Das erste Treffen fand am 28. September 2023 statt, an dem auch die Rollen und Verantwortlichkeiten mit den betroffenen Personen diskutiert wurden. Der Rollen- und Aufgabenbeschrieb der D&I-Verantwortlichen (Aufgabenprofile, Kompetenzen, Verantwortlichkeiten) wird im partizipativen Prozess mit den D&I-Verantwortlichen finalisiert und in der Folge von der Direktion verabschiedet. Angesichts der grossen Heterogenität der OE wird das GS SRD insbesondere die kleinen Einheiten bei der Ausübung der Aufgaben der D&I-Verantwortlichen stark unterstützen. Das GS JI hat ein Projekt über den Aufbau einer **Compliance-Organisation im Bereich D&I** in der JI geplant (Compliance D&I@JI). Dieses hat insbesondere zum Ziel, ein Compliance-Management-System (CMS) zu konzipieren und auf Direktionsebene zu verankern. Die konkreten Aufgabenprofile, die Kompetenzen und Verantwortlichkeiten der D&I-Verantwortlichen in den OEs werden in diesem Rahmen weiter konkretisiert. Die betroffenen Mitarbeitenden und Leitungspersonen werden dabei von Beginn an einbezogen. Dem weiteren Aufbau und Erhalt von Fachwissen wird ein grosser Stellenwert gegeben. Die Integration des Projekts in die Arbeiten für die Informationssicherheit sollte hierbei aktiv sichergestellt werden. Ebenso sollte der notwendige Ressourceneinsatz für dieses Projekt überprüft werden. Einzelne Massnahmen für die **Sensibilisierung** der Mitarbeitenden und Leitungspersonen wurden bereits ergriffen, wie zum Beispiel laufende Informationen im Intranet im Hinblick auf die Revision des IDG. Zudem wird dem Thema D&I in den verschiedenen Leitungsgremien sowie den Kaderdialogen grosse Aufmerksamkeit geschenkt. Mit der Revision des IDG sowie der Verordnungen wird sich für die meisten Mitarbeitenden in rechtlicher Hinsicht voraussichtlich nicht viel ändern. Die Chance wird jedoch genutzt, ein für die JI geltendes **Datenschutz-Risk-&-Compliance-Rahmenwerk** im partizipativen Prozess zu erstellen. Dieses soll die operative Umsetzung der

	Neuerungen sicherstellen sowie die Mitarbeitenden auf bereits heute bestehende Grundsätze weiter sensibilisieren. **Verzeichnis der Informationsbestände:** Bis auf eine kleine Fachstelle haben alle Organisationseinheiten der JI ein Verzeichnis über ihre Informationsbestände im Sinne von § 14 Abs. 4 IDG entsprechend der Zürcher Praxis auf ihren jeweiligen Websites aufgeschaltet. Diese wurden anhand einer Vorlage des GS JI im November 2023 zuletzt aktualisiert. Es ist darauf hinzuweisen, dass die Anforderungen an den Inhalt der Verzeichnisse im Rahmen der Anpassungen der IDV überprüft und allenfalls angepasst werden. Zudem wird die kantonale Verwaltung mit der IDG-Revision voraussichtlich verpflichtet, einen gemeinsamen, öffentlich zugänglichen Datenkatalog zu führen, der auch einen Überblick über sämtliche Datensammlungen und das Datenmanagement erlaubt. Der Regierungsrat soll hierzu eine Verordnung erlassen und die für die Führung des Datenkatalogs zuständige Stelle bezeichnen (vgl. § 44a E-OG RR, RRB Nr. 878/2023, S. 30 f. und S. 115 f.). Das GS JI wird durch entsprechende Vorlagen für eine einheitliche Umsetzung dieser Neuerungen in der JI sorgen. Eine grundlegende Überarbeitung der Verzeichnisse über die Informationsbestände in der JI scheint angesichts dieser Entwicklungen nicht prioritär.

2.2 Bearbeitung & Bekanntgabe von Informationen (Rechtliches)

Feststellungen	**Rechtsgrundlage:** Für die Bearbeitung von Personendaten ist eine entsprechende Rechtsgrundlage notwendig. Zumeist ist bei den Organisationseinheiten der JI eine explizite gesetzliche Grundlage für die Datenbearbeitung vorhanden. Diese ergibt sich aus den jeweiligen Spezialgesetzen. Die JI hat keine umfassende, direktionsweite Übersicht über die Datenbearbeitungen und die entsprechenden Rechtsgrundlagen. **Einwilligungen:** Darüber hinaus werden zum Teil in folgenden Fällen Datenbearbeitungen basierend auf Einwilligungserklärungen durchgeführt, wie beispielsweise in folgenden Bereichen: • Personensicherheitsprüfungen (JuWe-HR) • Umfragen durch F&E (MZU, Gefängnisse) • Um Informationen unverschlüsselt zu versenden, weil die Verschlüsselung z.T. nicht funktioniert (BVD-Lernprogramme «zu schnelles Fahren»)

	• Aktenbeizug: Entbindung von Schweigepflicht (KOH), Einbürgerungen (GAZ) • Videoaufzeichnungen zu Schulungszwecken (PPD), Sporttag mit Fotos (MZU) Für Einwilligungserklärungen sind keine direktionsweiten Vorgaben für einen formellen Gesamtprozess mit Abläufen, Zuständigkeiten, Einheitlichkeit, Aktualisierungsprozessen, Ablage, Auffindbarkeit etc. definiert. Ebenso bestehen keine Vorgaben, wie eventuelle Widerrufserklärungen gehandhabt werden sollen. **Datentransfers ins Ausland:** Datentransfers ins Ausland erfolgen meist einzelfallweise und auf Anfrage im Rahmen der Amtshilfe. Beispiele sind etwa die Übernahme von Bewährungshilfe durch ausländische Behörden bei der Durchführung der Bewährungsmassnahmen im Ausland (BVD) oder Nachbehandlungen in Kliniken im Ausland (PPD). Systematisch durchgeführte Datentransfers ins Ausland werden keine vollzogen. **Monitoring von Gesetzesänderungen:** Das Monitoring von Gesetzesänderungen in Bezug auf den Datenschutz und die Informationssicherheit ist in der JI nicht zentral organisiert. Die einzelnen Organisationseinheiten wählen verschiedene Vorgehensweisen. Das JuWe führt regelmässige Sitzungen im Fachbereich Recht durch, in welchen datenschutzrelevante Themen besprochen werden. Einige kleine Organisationseinheiten führen bezüglich D&I kein eigenständiges Monitoring durch und beziehen Informationen ausschliesslich über den GS-SRD (FK, FI).
Empfehlungen	Zur Übersicht empfehlen wir der JI auf Ebene Direktion die **Dokumentation der jeweiligen Rechtsgrundlage im Verzeichnis der Informationsbestände**. Zudem empfehlen wir, bei Datenbearbeitungen, zu denen **Einwilligungen** der betroffenen Personen eingeholt werden, zu **prüfen, ob sie IDG-konform sind**: • Die Abläufe sind zu definieren und die Verantwortlichkeiten im Zusammenhang mit der Einholung/Erteilung von IDG-konformen Einwilligungen festzulegen. • Bestehende Einwilligungen für eine Datenbekanntgabe oder Datenbearbeitung müssen auf IDG-Konformität hin überprüft werden. Ggf. braucht es eine Klärung, ob die Weiterleitung der Daten an Dritte wie z.B. an externe Forschende, Coaches von Lernprogrammen, IT-Provider etc. gestützt auf eine Einwilligung rechtmässig ist. Für den Fall, dass eine Einwilligung nicht IDG-konform erfolgt ist, ist dieser Mangel zu beheben. • Es empfiehlt sich zudem, jeweils zu prüfen, ob die Datenbearbeitung statt durch eine Einwilligung auch durch einen anderen Rechtfertigungsgrund erfolgen kann (z.B. gesetzliche Grundlage).

	• Da das geltende IDG keine expliziten Anforderungen an eine gültige Einwilligung stellt, empfehlen wir generell, sich an Art. 6 revDSG bzw. an den anerkannten Datenschutzgrundsätzen zu orientieren. • Für die Einwilligungsformulare empfehlen wir die Definition direktionsweiter Vorgaben und die entsprechende Anpassung bestehender Formulare. • Es braucht einen Prozess für den Widerruf gegebener Einwilligungen. Einwilligungen müssen gespeichert werden und über einen angemessenen Zeitraum auffindbar sein. Widerrufsmeldungen müssen den Aufbewahrungsfristen genügen. *Empfohlene Umsetzungsebene: Direktion und Organisationseinheit* Wir empfehlen bezgl. **Datentransfers ins Ausland**: • Kantonale Vorgaben zur Ergänzung bestehender bzw. zur Erstellung neuer Weisungen, Reglemente und Verträge hinsichtlich erlaubter und unerlaubter Datenübermittlungen ins Ausland sowie der hierfür einzusetzenden Übertragungsverfahren (z.B. Filetransfer). • Um eine Konformität mit dem revidierten IDG in jedem Fall sicher zu stellen, wird empfohlen, die Anforderungen gesamthaft auf das Niveau des revDSG anzuheben bzw. sich an den anerkannten Datenschutzgrundsätzen zu orientieren. *Empfohlene Umsetzungsebene: Kanton* Wir empfehlen der JI bezgl. **dem Monitoring von Gesetzesänderungen**: • ein **zentrales Monitoring von Gesetzesänderungen** mit besonderer Relevanz für den Datenschutz durch eine dedizierte Einheit in der Direktion zu etablieren (z.B. bei IDG-Revisionen oder der Schaffung bzw. Änderung von expliziten Rechtsgrundlagen für die Bearbeitung von Personendaten). • den einzelnen Organisationseinheiten zentral via GS-SRD und **Publikation** im Intranet all So wurden per Juli e relevanten Informationen zur Verfügung zu stellen. • eine via GS-SRD ausgeführte **zentrale Steuerung der Umsetzung** der Gesetzesänderungen, die für die gesamte oder wesentliche Teile der Direktion relevant sind (z.B. IDG-Revision). • einen **regelmässigen Austausch** zwischen den Organisationseinheiten der Direktion zu datenschutzrelevanten Gesetzesänderungen zu organisieren. *Empfohlene Umsetzungsebene: Direktion*

Stellungnahme & Massnahmen der JI	Die JI wird die empfohlenen *Massnahmen* umsetzen und sich – wo sinnvoll und empfohlen – für eine *kantonsweite* Umsetzung einsetzen (z.B. kantonale Vorgaben für den **Datentransfer ins Ausland**). Betreffend die **Einwilligung** in eine Datenbearbeitung ist darauf hinzuweisen, dass gemäss bundesgerichtlicher Rechtsprechung unter bestimmten Voraussetzungen in Grundrechtseingriffe eingewilligt werden kann (vgl. BGE 138 I 331 E. 6). So kennt das Datenschutzgesetz des Bundes das Instrument der Einwilligung als Rechtfertigungsgrund (Art. 6 Abs. 6 und 7, Art. 34 Abs. 4 Bst. b nDSG), und auch der Regierungsrat hat sich für entsprechende explizite Bestimmungen im zu revidierenden IDG ausgesprochen (vgl. §§ 12, 24 lit. c und 25 lit. c E-IDG; RRB Nr. 878/2023). Die Einwilligung in eine Datenbearbeitung kann namentlich auch zu mehr Transparenz und Selbstbestimmung über die eigenen Daten beitragen, auch wenn eine hinreichende Rechtsgrundlage (ohne Einwilligung) besteht. Dennoch sollen die heutigen Anwendungsfälle der Einwilligung erneut überprüft werden. In Bezug auf das **Monitoring von Gesetzesänderungen** ist auf den im Frühjahr 2023 neu geschaffenen **Fachbereich Informationen & Datenschutz im GS SRD** zu verweisen, mit dem der datenschutzrechtliche Wissensaufbau und -transfer in der Direktion verbessert werden soll. Der SRD wird künftig auch aktiver über relevante, die gesamte Direktion betreffende Gesetzesänderungen im Bereich D&I (namentlich IDG samt Verordnungen) informieren und die Umsetzung zentral steuern. Für die Umsetzung der Neuerungen aus dem totalrevidierten IDG samt Verordnungen wird der SRD ein Umsetzungskonzept erarbeiten. Die oben erwähnte CoP der D&I-Verantwortlichen wird bei der Umsetzung eine zentrale Rolle einnehmen.

2.3 Policy

Feststellungen	**Direktionsweite Policy** Die JI hat aktuell keine interne direktionsweite Policy für den Umgang mit Personendaten. Mit Blick auf die verschiedenen Organisationseinheiten, reicht die Bandbreite bezüglich Datenschutz-Policy oder analoger Vorgaben von spezifischen, abteilungsbezogenen und gesetzlich vorgeschriebenen Regelungen über Merkblätter eher informellen Charakters bis hin zu gar keinen Vorgaben zur konkreten und einheitlichen Umsetzung des Datenschutzes. **Beispiele sind:** • Leitfaden Datenschutz in den BVD (BVD) • Weisung Datenbekanntgabe (GAZ-Zivilstandswesen) • Weisung bzgl. der Nutzung von IncaMail (OJUGA)

Empfehlungen	Wir empfehlen die Erstellung **einer Datenschutz-Policy**, welche als Basisinformation für alle Mitarbeitenden gilt. Hilfreich wäre eine Sammlung sämtlicher relevanter Grundlagen zum Thema D&I. So soll der **Umgang mit Personendaten ganzheitlich angegangen** werden. Inhaltlich empfehlen wir der JI mindestens die folgenden Themen damit abzudecken: Governance, Rollen und Verantwortlichkeiten, Geltungsbereich der relevanten Gesetze, anerkannte Datenschutzgrundsätze der Bearbeitung, Übermittlungen (Weitergabe von Personendaten), Betroffenenrechte, Datenschutzvorfälle, technische und organisatorische Massnahmen, Schulung und Bewusstseinsbildung, Notfallmassnahmen bzw. Business Continuity Management (BCM). **Interne Weisungen**, Policies und Richtlinien **sowie** die jeweiligen **Kontrollen sind** zum gegebenen Zeitpunkt den jeweiligen Anforderungen des sich in Revision befindlichen **IDG anzupassen.** Zudem empfehlen wir, diese Weisungen und Hilfsmittel allenfalls pro Organisationseinheit durch Vorgaben aus den Spezialgesetzen zu ergänzen. Bei der Ausgestaltung der Weisungen, Policies und Richtlinien empfehlen wir, sich am «State of the Art» für vergleichbare Organisationen zu orientieren. *Empfohlene Umsetzungsebene: Direktion und Organisationseinheit*
Stellungnahme & Massnahmen der JI	Die JI wird die Empfehlung zur Erstellung einer Datenschutz-Policy im Rahmen des Rollouts des Digitalen Arbeitsplatzes (DAP) umsetzen. Inhaltliche Teilgehalte der Policy existieren bereits bzw. sind beim SRD in Arbeit. Die Arbeiten sind zum Teil weit fortgeschritten (z.B. Rollen und Verantwortlichkeiten D&I-Verantwortliche, 1x1 des Datenschutzes für die Mitarbeitenden inkl. Geltungsbereich der relevanten Gesetze und anerkannte Datenschutzgrundsätze), andere wurden im Sommer 2023 initiiert (z.B. direktionsweite Governance, Massnahmen in den Bereichen Schulung und Bewusstseinsbildung sowie Business Continuity Management (BCM)). Die Anpassung der verschiedenen internen Weisungen, Policies und Richtlinien an das revidierte IDG wird als Teil des auszuarbeitenden Umsetzungskonzepts angegangen und zentral überprüft.

2.4 Datenmanagement

Feststellungen	**Datenqualität:** Es gibt zwar keine spezifische, direktionsweite schriftliche Weisung oder Vorgabe zur Sicherung der Datenqualität, es werden jedoch von den einzelnen Organisationseinheiten der JI Massnahmen durchgeführt, welche zur Sicherstellung der Datenqualität und Aktualität beitragen. Beispiele sind systemisch erzwungene Mechanismen (z.B. Muss-Felder im Vitomed, Einspeisen von Feldern via RIS1/2 Schnittstelle), aber auch die Zertifizierung von Prozessen, wie etwa ISO 9001 für das Qualitätsmanagement im Therapieprozess, wobei Updates zur

	Krankengeschichte im Vitomed alle 3 Monate von Qualitätszirkelleitenden kontrolliert und unterschrieben werden (PPD). Unsere Ansprechpersonen stellten fest, dass teilweise eine Diskrepanz zwischen den Daten im System und den physischen Akten (BVD, SHA-ZH) besteht. Das Primat liegt vor allem in den von Gesetzes wegen schriftlich geführten Verfahren bei den Papierakten. Das hat zur Folge, dass in diesen Bereichen die Angaben im System nach Abschluss eines Geschäfts meist nicht mehr aktualisiert werden. Ebenso kommt es vor, dass Datenaktualisierungen, welche nicht an laufende Geschäfte gekoppelt sind, ausserhalb der Systeme stattfinden (z.B. MZU-Stammdatenblatt, ausserhalb des RIS). Somit besteht kein Prozess, der definiert, wie die Systemdaten aktuell gehalten werden sollen. Prozesse, Kontrollen oder Regelungen, die sicherstellen, dass bei der Datenerhebung nur Daten erfasst bzw. bearbeitet werden, welche für den rechtmässigen Zweck zwingend notwendig sind, bestehen ebenfalls noch nicht. **Aufbewahrung:** Alle Organisationseinheiten der JI kommen ihrer Pflicht zum Anbieten ihrer Akten ans Staatsarchiv (StAZH) gemäss IDG grundsätzlich nach. Die Aufbewahrung von Informationen und das Anbieten an das Staatsarchiv nach Ablauf der Frist werden von den Organisationseinheiten der JI jedoch unterschiedlich gehandhabt. Teilweise bestehen hierzu feste Zuständigkeiten (z.B. Admin im GS-SRD, Qualitätsverantwortliche im JuWe), und es sind feste Zyklen mit dem StAZH abgemacht. Ebenso sind zum Teil Vorgaben oder eine Vereinbarung mit dem StAZH hinsichtlich der Archivwürdigkeit von Informationen (z.B. BVD) vorhanden. Jedoch gibt es auch Organisationseinheiten, welche schon länger keinen Archivierungszyklus mehr durchlaufen haben (z.B. MZU, BRK/SHA Dietikon, BRK Winterthur), oder bei denen keine regelmässigen Archivierungszyklen definiert sind (z.B. SHA-ZH). Die jeweiligen Gründe herfür wurden in der Umfrage nicht einzeln erhoben. Einigen Ansprechpartnern war es nicht klar, ob die elektronisch gespeicherten Informationen archiviert werden - und wenn ja, wie sie archiviert werden (z.B. RIS im JuWe; InfoSys bei der KOH). **Löschen / Vernichten:** Zum Entsorgen von physischen Informationen, welche die Aufbewahrungsfrist überschritten haben und nicht archivwürdig sind, werden DataRec Container verwendet. Elektronische Informationen werden aber nicht systematisch gelöscht. Beispielsweise wurden die ca. 25-jährigen RIS1-Daten vor sieben Jahren ins RIS2 migriert und sind dort noch vorhanden. Vermutlich sind diese älteren Daten nicht systematisch im System identifizierbar und müssten deshalb manuell gelöscht werden. Im RIS2 wurden bisher keine Daten gelöscht. Ein expliziter, generell gültiger Löschprozess fehlt. Eine technische Lösung für ein regelmässiges Löschen nach Ablauf der Aufbewahrungsfristen liegt nicht vor. Eine solche Lösung wäre technisch vermutlich möglich. Wie sie konkret umgesetzt werden müsste (z.B. im Hinblick auf Backups, unstrukturierte Datensammlungen, Cloud-Lösungen etc.), ist jedoch noch nicht klar.

Empfehlungen	Zur **Sicherstellung der Datenqualität** sind die folgenden Massnahmen auf Ebene Direktion zu implementieren: • Erstellung von Weisungen und Prozessbeschreibungen. • Regelmässige Erinnerung der Mitarbeitenden und/oder betroffenen Personen, ihre Datensätze zu überprüfen. Zusätzlich sollen bei der Einführung oder der **Optimierung von Applikationen** jeweils die folgenden technischen Massnahmen in Betracht gezogen werden: • Festlegen anzuwendender Datenqualitätskriterien • Datenqualität bei Erfassung prüfen (gegenüber Qualitätskriterien) • Datenverifikation durch System • Datenspeichervorgaben (z.B. Pflichtfelder / automatische Vorschläge «by Default») • Regelmässige Überprüfung der Datenqualität (z.B. Prüfung der Stammdaten durch Fallverantwortliche) *Empfohlene Umsetzungsebene: Kanton und Direktion (je nach Applikationen)* Um zu vermeiden, dass Daten entgegen dem **Datenminimierungsprinzip** über ihren Zweck hinaus bearbeitet werden, empfehlen wir zudem folgende Massnahmen: • Prüfung, ob eine spezifische Weisung und damit zusammenhängende Kontrollen für einzelne Systeme erstellt werden sollten, in denen u.a. darauf hingewiesen wird, welche Daten i.S. der Datenminimierung erfasst resp. nicht erfasst werden dürfen. • Die Verwendung von optionalen Daten und Freitextfeldern ist auf das absolut Notwendige einzuschränken und dann mit klaren Anweisungen zu versehen, welche Daten erwartet werden. • Des Weiteren empfehlen wir, die Mitarbeitenden entsprechend zu schulen und deren Bewusstsein zum Thema Datenqualität zu schärfen. *Empfohlene Umsetzungsebene: Kanton, Direktion und Organisationseinheit (je nach Zuständigkeit für Applikationen)* Wir empfehlen, generell geltende **Vorgaben zur Aufbewahrung** (bzw. zur Archivwürdigkeit, zu Archivierungszyklen, etc.) von Informationen auf Kantonsebene nicht nur zu definieren, sondern diese Vorgaben auch regelmässig zu kommunizieren. Diese Massnahme scheint uns aufgrund der z.T. langen Archivierungszyklen und dem Wechsel von Mitarbeitenden angezeigt. Dass die spezifischen, für die einzelnen Organisationseinheiten geltenden Archivierungsvorgaben eingehalten werden, sollten die betreffenden Einheiten selbst sicherstellen. Bestehende Weisungen zur Aufbewahrung sind nach der Inkraftsetzung des kommenden, revidierten IDG zu konkretisieren, zu überprüfen und anzupassen.

	<u>Empfohlene Umsetzungsebene:</u> Organisationseinheit Es sind **angemessene Löschprozesse** und Zuständigkeiten für elektronisch gespeicherte Daten zu definieren. So ist sicherzustellen, dass nicht mehr benötigte und nicht (mehr) aufbewahrungspflichtige elektronische Daten regelmässig gelöscht werden. *<u>Empfohlene Umsetzungsebene:</u> Organisationseinheit* Die vorhandenen **Weisungen und Reglemente** sind hinsichtlich IDG-Anforderungen zu prüfen und ggf. anzupassen. *<u>Empfohlene Umsetzungsebene:</u> Direktion und Organisationseinheit*
Stellungnahme & Massnahmen der JI	Die JI wird die empfohlenen Massnahmen umsetzen und sich in den direktionsübergreifenden Bereichen für eine kantonsweite Umsetzung einsetzen (z.B. betr. IT-Grundversorgung oder im Rahmen der sog. Strategischen Initiativen gemäss der kantonalen Digitalisierungsstrategie „gemeinsam digital unterwegs“ betr. Data Governance/Datenarchitektur). Die JI setzt die Grundsätze der **Informationssicherheit und Privacy by Design** wann immer möglich um. Sie setzt sich dafür ein, dass entsprechende Architekturprinzipien kantonsweit zur Anwendung kommen. Wo dies nicht möglich ist, soll die Grundsätze namentlich durch die Etablierung einer Community of Practice, die Schulung von Mitarbeitenden sowie geeigneten Weisungen und Hilfsmittel gewährleistet werden. Die Kompetenz beim Umgang mit Daten als eine der Kernkompetenzen in diesem Feld, wird im Rahmen der Strategischen Initiative für die gesamte Kantonsverwaltung gefördert. Die Strategische Initiative „Organisation“ (SI Organisation) ist mit der Entwicklung der Digital Skills beauftragt. Die Strategische Initiative „Daten“ (SI Daten) wird ein Schulungsangebot zum Umgang mit Daten beisteuern. Zudem startet aktuell in der SI Organisation ein Projekt zur kantonsweiten Homogenisierung der Geschäftsfallbearbeitung. Die JI setzt sich dafür ein, dass die oben genannten Themen in den laufenden Projekten berücksichtigt werden. Wo immer möglich, soll die **Datenqualität** direkt bei der Dateneingabe in den Fachapplikationen sichergestellt werden. Dies kann kantonsweit über die zurzeit in Erarbeitung befindlichen Architekturprinzipien geschehen (Projekt Architekturmanagement ZH). Die JI setzt sich dafür ein, dass entsprechende Prinzipien aufgenommen werden. Ferner sollen in einem zweiten Schritt im Rahmen der Strategischen Initiative „Daten“ Massnahmen zur Sicherstellung der Qualität von Daten erarbeitet werden. Das **Datenminimierungsprinzip** respektive die Datensparsamkeit ist ein Grundsatz des Datenschutzes, dem die Kantonale Verwaltung verpflichtet ist (IDG). Diesem Prinzip soll in den Fachapplikationen über die Architekturprinzipien und darüber hinaus in den Grundlagen zur Datenbewirtschaftung („Data Governance“) Nachdruck verliehen werden. Das betrifft auch nicht mehr notwendige Daten. Diese Daten sowie Daten, welche keiner Aufbewahrungspflicht (mehr) unterstehen, sollen möglichst schnell gelöscht oder anonymisiert werden. Um dieses Ziel zu erreichen, strebt die JI an, die Aufbewahrungsfrist von Daten im zu erarbeitenden

	Datenkatalog zu hinterlegen (Data Life Cycle). Dies wird es erlauben, die zuständigen Stellen automatisiert an eine **Löschung respektive Archivierung** der Daten zu erinnern. Der Regierungsrat hat einen entsprechenden Datenkatalog in der Totalrevision des IDG dem Kantonsrat vorgeschlagen.

2.5 Risikomanagement & Kontrolle

Feststellungen	In der JI besteht kein direktionsweites **Risikomanagement von D&I.** Im JuWe verfügen die Vollzugseinrichtungen je einzeln über ein solches Risikomanagement, allerdings ist dort der Fall einer Datensicherheitsverletzung nicht berücksichtigt. **DigiSol** ist derzeit daran, für die JI **ein Informationssicherheitsrisikoregister** (Digital Security Control Center) aufzubauen. Dieses Register soll auch den Schutzbedarf für Applikationen und Systeme bestimmen. Bei einigen Systemen ist die Business Continuity sichergestellt, so z.B. bei Elektra (elektronische Krankenakten). Dort ist auch ein dokumentierter Notfallzugriff, z.B. bei Stromausfall, möglich. **Audits** fanden **bisher nur bei der DigiSol** im Rahmen von Sicherheitsaudits statt. Zudem wurden vereinzelt Penetrationstests durchgeführt (OSTA, 2023). Im Rahmen der Tätigkeiten der kantonalen Datenschutzbeauftragten wurden ausserdem entsprechende Reviews durchgeführt (z.B. KEP, 2020; MZU, 2023). Ansonsten fanden bei den Organisationseinheiten der JI keine Audits mit Fokus auf D&I statt.
Empfehlungen	Wir empfehlen der JI, ein direktionsweites **Risikomanagement** aufzubauen, Massnahmen und Kontrollen zu definieren und klar zugewiesene Rollen, Verantwortlichkeiten und Ansprechstellen festzulegen, um beispielsweise bei Datensicherheitsverletzungen effizient und effektiv reagieren zu können. *Empfohlene Umsetzungsebene: Direktion* Wir empfehlen zudem, **periodische Audits** oder Reviews sowohl auf Stufe Generalsekretariat wie auch in den einzelnen Organisationseinheiten durchzuführen und die Ergebnisse angemessen zu dokumentieren. Sodann ist sicherzustellen, dass die im Audit erkannten Befunde von der betroffenen Stelle angegangen und allfällige Datenschutzlücken geschlossen werden. Hierzu ist die Einflussnahme der Amtsleitung gefordert. Zudem müssen die Prüfungen angepasst bzw. erweitert werden, wenn sich bei den Massnahmen, die es zu überwachen gilt, etwas geändert hat. *Empfohlene Umsetzungsebene: Direktion und Organisationseinheit*
Stellungnahme & Massnahmen der JI	Derzeit wird in der JI eine **Community of Practice «Security»** aufgebaut, bestehend aus dem Sicherheitsbeauftragten der JI sowie Vertreterinnen und Vertretern aus allen Organisationseinheiten (**D&I-Verantwortliche**). Das erste Treffen fand im September 2023 statt. Die Risiken wurden zwischenzeitlich evaluiert. Das **Risiko-Register** für Fachapplikationen und Systeme ist im DSC2 Tool und Excel abgebildet. Die erforderlichen Massnahmen für die bereits bestehenden Risiken sind geplant. Neu werden zusätzliche Risikoanalysen (gemäss BSIR) in den Projekten oder auf Stufe OEs mit Hilfe des Tools DSC2 durchgeführt.

	Zudem soll eine Übersicht über **Schutzbedarfs -und Risikoanalysen** erstellt und so weit als nötig nacherarbeitet werden. Die neu geplanten Risikoanalysen sollen den Bereich Audit abdecken. Im Übrigen ist darauf hinzuweisen, dass die JI in engem Austausch mit der Datenschutzbeauftragten des Kantons Zürich steht.

2.6 Privacy b Design / Privacy by Default

Feststellungen	**„Privacy by Design“** bzw. Datenschutz durch Technik und **„Privacy by Default“** bzw. Datenschutz durch datenschutzfreundliche Voreinstellungen sind aktuell noch nicht in der gesamten JI gemäss den Anforderungen des aber erst kommenden IDG d.h. gemäss den anerkannten Datenschutzgrundsätzen, verbreitet. In der ganzen JI wird der Hermes-Projektmethodologie gefolgt, die auch verschiedene Instrumente zur Gewährleistung des Datenschutzes und der Informationssicherheit beinhaltet (u.a. Rechtsgrundlagenanalyse, Datenschutzfolgeabschätzung (DSFA), Schutzbedarfsanalyse, ISDS-Konzept). In der vorliegenden Erhebung konnte nicht umfassend geprüft werden, wie in der Direktion und insbesondere bei DigiSol mit diesen Instrumenten umgegangen wird. Wir können nur auf die Wichtigkeit hinweisen, dass der Datenschutz in den Projekten tatsächlich stets konsequent berücksichtigt wird und dass insbesondere bei Projekten unter der Leitung der DigiSol die jeweiligen Amts- und Fachstellen oder der GS-SRD als Kompetenzstelle für den Datenschutz involviert werden. **Datenschutzfolgenabschätzungen [DSFA]** werden noch nicht konsequent bei allen neuen Vorhaben durchgeführt. Gewisse Einheiten wie die DigiSol führen solche jedoch stets im Rahmen von Hermes-Projekten anhand der Vorlagen der Datenschutzbeauftragten des Kantons Zürich durch (z.B. bei der Einführung von Simed), ebenso das Staatsarchiv (z.B. im Projekt DigDataZH). Es wäre der Vollständigkeit halber mittels zusätzlicher Erhebungen zu prüfen, ob die DSFA in den Organisationseinheiten gemäss den Anforderungen des IDG durchgeführt und dokumentiert werden und inwiefern namentlich bei Projekten unter der Leitung von DigiSol das GS – oder andere Amtsstellen als Auftraggeber – eingebunden werden sollen. Weiter könnte man prüfen, inwiefern unter den Mitarbeitenden in den Organisationseinheiten bekannt ist, wann und wie sie eine DSFA durchführen müssen sowie ob und wie die korrekte Durchführung der DSFA kontrolliert wird. Ebenfalls in der vorliegenden Erhebung nicht geprüft wurde die Frage, ob die gemäss IDG vorgesehene Vorabkontrolle bei der Datenschutzbeauftragten des Kantons Zürich konsequent durchgeführt wird, sofern eine beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für die Grundrechte der betroffenen Personen einhergeht.

Empfehlungen	Für alle prozessrelevanten oder technischen Änderungen und Neuimplementierungen braucht es einen **„Privacy by Design“**-Prozess, bei welchem die Datenschutzaspekte von Beginn an berücksichtigt und dokumentiert werden. Ebenso braucht es Prozesse bzw. Massnahmen, welche die Umsetzung des Grundsatzes **„Privacy by Default“ sicherstellen**, z.B. bei Updates oder Neueinführung von IT-Systemen. Wir empfehlen, diese Prozesse **kantonal** gesamtheitlich zu definieren. *Empfohlene Umsetzungsebene: Kanton* Dies betrifft auch die IT-Projektmethodik (HERMES). Insbesondere bei bereits anberaumten oder gestarteten Projektvorhaben (z.B. bei den 15 Digitalisierungsprojekten im JuWe mit dem neuen RIS, dem SmartPrison etc.), sollen diese Grundsätze anhand direktionsweiter Vorgaben berücksichtigt werden, solange keine gesamtkantonalen Vorgaben bestehen. *Empfohlene Umsetzungsebene: Direktion* Bei der Einführung neuer Systeme, Prozesse oder Verfahren, welche aufgrund der darin bearbeiteten Personendaten potenziell die Grundrechte der betroffenen Personen tangieren können, muss durch die JI bzw. durch die für den Prozess Verantwortlichen eine **Datenschutzfolgenabschätzung durchgeführt werden**. Dies nicht nur bei IT-Projekten. Hierzu muss den Mitarbeitenden aller Organisationseinheiten bekannt gemacht werden, welche Verantwortlichkeiten bestehen und welche Kriterien und Risiken bei der Durchführung einer DSFA berücksichtigt werden müssen. Die Zuständigkeit ist klar zu regeln. Sinnvollerweise ist die Datenschutzfolgeabschätzung bei Projekten unter der Leitung der DigiSol in Zusammenarbeit mit den betreffenden Organisationseinheiten zu erstellen. Der oder die jeweilige D&I-Verantwortliche sollte die OE und DigiSol bei der Durchführung unterstützen und die involvierten Personen entsprechend schulen. *Empfohlene Umsetzungsebene: Direktion*
Stellungnahme & Massnahmen der JI	In der kantonalen Verwaltung sind Projekte verpflichtend nach der **HERMES-Methode** zu führen. Diese sehen die für den Datenschutz und die Informationssicherheit notwendigen Prüfschritte zwingend vor (insb. Rechtsgrundlagenanalyse, Datenschutzfolgeabschätzung, Schutzbedarfsanalyse, ISDS-Konzept, allfällige Vorabkontrolle bei der Datenschutzbeauftragten des Kantons Zürich). Die Erfahrung hat jedoch gezeigt, dass die Verantwortlichkeiten und Zusammenarbeit z.B. zwischen den Organisationseinheiten der IT (DigiSol) und dem SRD nicht immer klar sind. Der SRD ist deshalb seit Frühsommer 2023 daran, unter Mitwirkung der DigiSol und sowie in Absprache mit der DSB einen **Musterprozess** samt Verantwortlichkeiten zu definieren, sowohl für Projekte mit als auch ohne IT-Bezug. Dieser soll im Q4 2023 für die gesamte Direktion verbindlich gelten und angemessen kommuniziert werden. In technischer Hinsicht ist darauf hinzuweisen, dass die **IT-Grundversorgung durch das Amt für Informatik (Finanzdirektion)** für

	die gesamte kantonale Verwaltung bereitgestellt wird. Die JI setzt sich dafür ein, dass die Grundsätze Privacy by Design und Privacy by Default im Rahmen der IT-Grundversorgung berücksichtigt werden und auch entsprechende technische und organisatorische Massnahmen getroffen werden (z.B. Prozesse, Voreinstellungen etc.). Neu soll mit Einführung des DAPs die Sicherheitslösung «Purview» mitgeliefert werden. In Purview können Kriterien erfasst werden, nach denen Datensätze zwingend und hochgradig automatisiert einer bestimmten Kategorie (z.B. «öffentlich» oder «vertraulich») zugeteilt werden. Jeder Kategorie können wiederum vordefinierte Schutzmassnahmen wie z.B. der Aufdruck des Wortes «Vertraulich» in der Fusszeile oder eine zwingende Verschlüsselung des Datensatzes aufgeprägt werden. Die entsprechenden Schutzmassnahmen werden dann bei Aufruf oder Speicherung eines Datensatzes automatisch durch das System ausgeführt. Somit besteht die Möglichkeit, Informationen einschliesslich Personendaten nach dem Ansatz «Privacy by Design» zu klassifizieren und entsprechend zu schützen. Die Mitarbeitenden werden mittels geeigneter Hilfsmittel wie Merkblätter, einem Schulungsvideo sowie durch einheitsspezifische Einführungsprozesse befähigt, die von ihnen bearbeiteten Informationen entsprechend ihrer Vertraulichkeit konsequent und einfach zu klassifizieren und zu verschlüsseln. Mittels Voreinstellungen je nach Informationsart wird dem Grundsatz des Privacy by Default Rechnung getragen. Schliesslich ist darauf hinzuweisen, dass die Grundsätze «Privacy by Design» und «Privacy by Default» gemäss Entwurf des Regierungsrates explizit im IDG verankert werden sollen (vgl. § 30 Abs. 2 und 3 E-IDG; RRB Nr. 878/2023).

2.7 Sicherheitsmassnahmen

Feststellungen	Zur Sicherstellung der IT-Sicherheit sind verschiedene **technische sowie organisatorische Massnahmen** implementiert worden. So bestehen beispielsweise von der DigiSol Richtlinien zu Klassifikation von Informationen. Ende Q2 2023 soll zudem der Microsoft Purview Pilot fertig sein (Stand zum Zeitpunkt der sog. «Deep Dives», d.h. der Vertiefungsinterviews). **Zugriffsberechtigungen** werden durch Passwörter geschützt und der Zugriff gewisser Bereiche wird auf einen spezifischen Personenkreis eingegrenzt. Es bestehen Berechtigungskonzepte für die zehn kritischsten Fachapplikationen. Bei den meisten Organisationseinheiten werden jedoch Berechtigungen gemäss Musterpersonen («gleich wie der Vorgänger») vergeben. Damit besteht bei den jeweiligen Ämtern und Fachstellen (bzw. den jeweiligen Vorgesetzten) oft keine Übersicht über die effektiv erteilten Berechtigungen. Auch die DigiSol hat keine solche Übersicht.

	Weiter ist die **Zuständigkeit** für Massnahmen und deren Umsetzung fragmentiert. Zum Teil ist die Zuständigkeit kantonal geregelt (z.B. Endpoint Protection durch das AFI), zum Teil nur bei der Direktion (eigene Infrastruktur der DigiSol). Auch innerhalb der DigiSol zieht sich diese Fragmentierung weiter, etwa bei der IT-Sicherheitsarchitektur welche bei den Sicherheitsarchitekten der DigiSol angesiedelt ist, ohne Einwirken oder Konsultation des ISID.
Empfehlungen	Die Direktion sollte überprüfen, ob bei Vorhaben die bestehenden Sicherheitskonzepte und -massnahmen eingehalten und dem Risiko entsprechend umgesetzt werden. Ganz besonders sollten hierbei in allen Bereichen die **Zugriffsrechte** auf Personendaten im Sinne des IDG **auf das notwendige Mass («Need to know»-Prinzip) eingeschränkt werden**. Hierfür sind nach dem Vorbild der bereits bestehenden Konzepte entsprechende **Weisungen und Berechtigungskonzepte** zu erstellen und ein kontinuierliches **Berechtigungsmanagement** / Benutzerberechtigungssystem aufzubauen. Wir empfehlen darüber hinaus, die **Mitarbeitenden** zu **sensibilisieren** und per Policy oder **vertraglich** zu **verpflichten**, für den Versand von Personendaten nur die offiziell zugelassenen Verfahren zu verwenden (z.B. Verschlüsselung beim Datentransfer). *Empfohlene Umsetzungsebene: Direktion und Organisationseinheit*
Stellungnahme & Massnahmen der JI	Bei allen Projekten und Schutzobjekten wird der **Schutzbedarf** eingestuft und anschliessend über die Notwendigkeit eines Sicherheitskonzepts (ISDS) entschieden. Bei der Erstellung des Sicherheitskonzepts wird eine Risikoanalyse durchgeführt. Entsprechend werden zusätzliche Massnahmen beschlossen, oder das Risiko wird ins Register aufgenommen. Für die 10 wichtigsten Fachapplikationen wurde ein Entwurf für die **Berechtigungskonzepte** erstellt. Im Moment werden die Berechtigungskonzepte risikobasiert nach Relevanz der jeweiligen Applikationen mit externer Unterstützung erarbeitet. Die Mitarbeitenden der STA.ZH werden aktuell mit einer **Schulung** zum Umgang mit Daten und USB-Speichermedien geschult. Mit der Einführung des DAP und mittels der durch «Purview» bereitgestellten, deutlich verbesserten Identity & Access Management (IAM) Funktionalitäten können die Zugriffsberechtigungen stark verbessert aufgesetzt werden. Zugriffsrechte der Benutzenden können dann nach aktuellen Prinzipien (z.B. rollenbasiert, zeitlich eingeschränkt, zusätzlich gesichert, etc.) optimiert werden. Das „Need to know“-Prinzip sowie die Informationssicherheit können damit technisch wie organisatorisch besser entsprechend der jeweiligen Risiken gewährleistet werden. Die Einführung des DAPs wird auch mit einer Datenschutz-Policy bzw. Weisung sowie mit Schulungsmassnahmen begleitet (vgl. oben).

2.8 Drittparteienmanagement

Feststellungen	Bei der JI haben in fast allen befragten Bereichen Drittparteien Zugriff auf Personendaten der JI. Geheimhaltung ist generell zum einen im Rahmen von standardisierten Vertragsbestimmungen geregelt, zum andern werden Geheimhaltungserklärungen eingeholt (z.B. bei externen Projektmitarbeitenden). Auftragsbearbeitungsverhältnisse mit Outsourcing-Providern sind vertraglich geregelt. Die Standardverträge der DigiSol wurden gemäss Vorgaben bzw. Merkblatt der kantonalen Datenschutzbeauftragten erstellt und beinhalten das Einholen von Geheimhaltungserklärungen und einen Personensicherheitsüberprüfungsprozess. Die jeweiligen DigiSol Projektleitenden sind verantwortlich für die Prüfung und ggf. das Unterbreiten des Vorhabens zur Vorabkontrolle durch die kantonale Datenschutzbeauftragte (z.B. bzgl. des Hostings in der Ametic-Cloud von Simed). Teilweise finden jedoch auch Auftragsdatenbearbeitungen ausserhalb des Aktionskreises der DigiSol statt. Beispiele sind: • SOS-Ärzt*innen: Diese haben Zugriff auf die Medikamenten-Karte, ohne Vitomed (PPD) • PUK: Hat Zugriff auf die JI-Systeme, inkl. Vitomed (PPD) • Zusammenarbeit mit einem externen Anwalt (JuWe-HR) oder PR-Agentur (Kommunikationsabteilung) • GAZ-Applikationen FAE und E-Einbürgerungen, gehostet von Bedag Informatik AG (GAZ) Das JuWe überarbeitet derzeit seine AGB sowie die Standardverträge. In den unteren zwei Fällen bestehen keine standardisierten vertraglichen Regelungen, bzw. ist unklar, inwieweit datenschutzrelevante Themen (z.B. Anforderungen an die Datensicherheit) in den jeweiligen Verträgen berücksichtigt wurden. Es finden ausserdem keine externen Audits bei Auftragsbearbeitern statt. Zum Zeitpunkt der Befragungen bestanden noch keine direktionsweiten Vorgaben zur Auswahl von Drittparteien (z.B. ISO-Zertifizierungen, bestehende technische und organisatorische Massnahmen) und es wurde noch nicht der ganze Lebenszyklus der Auftragsdatenbearbeitungen (insbesondere regelmässige Reviews/Audits und Offboarding) berücksichtigt. Die JI war jedoch bereits damit befasst, die entsprechenden direktionsinternen Vorgaben zu aktualisieren und zu überarbeiten.

Empfehlungen	Wir empfehlen der JI: • Bestehende und neue **Verträge** zur Auftragsbearbeitung hinsichtlich **Konformität** mit den jeweils relevanten datenschutzgesetzlichen Anforderungen **zu prüfen** und gegebenenfalls **anzupassen**. Dabei empfehlen wir, sich an den anerkannten Datenschutzgrundsätzen zu orientieren. Standards wie z.B. diejenigen des revDSG, der ISO oder der EU-DSGVO helfen, juristische Massnahmen wie Standard-Vertragsklauseln oder technische und organisatorischen Massnahmen rasch festzulegen und umzusetzen. • Die JI soll die **Prozesse und Verantwortlichkeiten** im Zusammenhang mit der Unterzeichnung von Geheimhaltungserklärungen durch Drittparteien, die potenziell Zugriff oder Einsicht in Personendaten der JI haben, einheitlich **definieren und umsetzen**. • Zudem soll ein Prozess eingeführt werden, durch welchen die Einhaltung dieser Vorgaben regelmässig **kontrolliert** wird. • Des Weiteren sind die Definitionen und **Bestimmungen** in den Verträgen und Vertragsbestandteilen hinsichtlich (revidierter) Datenschutzgesetzgebung des Kantons Zürich zu **aktualisieren**. • Schliesslich hat vor Vertragsabschluss sowie (bei laufenden Verträgen) während der Vertragslaufzeit eine Überprüfung der Datenschutz- und Datensicherheitsmassnahmen der Auftragsbearbeiter zu erfolgen. Solche **Audits** sollten zentral dokumentiert werden. Für den Fall festgestellter Lücken ist auf eine Vertragsanpassung und/oder Ergänzung hinzuwirken, um die IDG-Anforderungen bzw. die Anforderungen des Schweizer Datenschutzgesetzes zu erfüllen. *<u>Empfohlene Umsetzungsebene:</u> Direktion*
Stellungnahme & Massnahmen der JI	Die JI hat die Notwendigkeit einer **Verbesserung ihres Drittparteienmanagements** erkannt und strebt zu diesem Zweck vordringlich die Schaffung **direktionsinterner Vorgaben und Prozesse** an. Dabei steht die Konkretisierung von § 6 IDG und § 25 IDV im Zentrum, unter Berücksichtigung der Vorgaben der DSB zu standardvertraglichen Regelungen und Geheimhaltungserklärungen. Ziel ist es aber auch, die juristische und organisatorische Komplexität dieses Themenbereichs zu reduzieren, grössere Verbindlichkeit und klare Zuständigkeiten zu schaffen sowie die Mitarbeitenden verstärkt für problematische Aspekte des Bearbeitens im Auftrag zu sensibilisieren. Die entsprechenden Arbeiten sind weit fortgeschritten; es kann mit einer Umsetzung im Q1 2024 gerechnet werden. Sobald die direktionsinternen Vorgaben und Prozesse festgelegt sind, werden auch die bestehenden Verträge mit Dritten entsprechend überprüft. Weitere Massnahmen – insbesondere zur **technischen Unterstützung des Drittparteienmanagements auch auf Kantonsebene** – sind derzeit in Abklärung: Vertragsverwaltung DigiSol, Aktualisierung Sicherheitsdatenbank, Überarbeitung BISR 22 und entsprechende

	Services. Ein konkreter Umsetzungstermin lässt sich diesbezüglich noch nicht nennen.

2.9 Betroffenenrechte

Feststellungen	**IDG-Gesuche:** Das Verfahren, die Zuständigkeit sowie die Gewährung von Gesuchen nach § 20 Abs. 2 IDG (Zugang zu den eigenen Personendaten) sowie § 21 IDG (Gesuche zum Schutz der Persönlichkeit) sind gesetzlich geregelt (IDG, IDV, subsidiär VRG; insb. §§ 16 ff. IDV). Je nach Organisationseinheit bestehen hierzu weitere Konkretisierungen oder Umsetzungshilfen. Zum Beispiel beim JuWe-HR bestehen für die Bearbeitung solcher Gesuche ein schriftlich dokumentierter Ablauf und feste Zuständigkeiten. Nicht überall besteht zusätzlich zu den Vorgaben gemäss IDV ein formalisierter Prozess und die Zuständigkeit ist nur informell bekannt (z.B. im MZU). Beim Grossteil der Organisationseinheiten werden IDG-Gesuche via Rechtsdienst abgewickelt. Organisationseinheiten ohne eigene juristische Fachpersonen werden vom GS SRD unterstützt. **Algorithmische Entscheidsysteme:** Im JuWe werden teilweise Tools zur automatisierten Unterstützung von Entscheidungsprozessen verwendet. Die folgenden Beispiele wurden genannt: • ROS: Risikoorientierter Sanktionenvollzug • FOTRES: Forensisches Operationalisiertes Therapie-Risiko-Evaluations-System Der Review der Auswertungen obengenannter Tools findet zwar jeweils durch den Fallverantwortlichen statt, das heisst der Entscheidungsprozess ist nicht komplett automatisiert. Mit den gespeicherten Daten ist es grundsätzlich jedoch möglich, ein Profiling (automatisierte Auswertungen von Informationen, um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen, gemäss § 3 Abs. 4 lit. c IDG) vorzunehmen. Bei den anderen Organisationseinheiten findet kein Profiling statt.
Empfehlungen	**Gesuche um Zugang zu den eigenen Personendaten** (§ 20 Abs. 2 IDG): • Die **Prozesse** im Zusammenhang mit IDG-Gesuchen sowie die Form und der Umfang der Auskunftserteilung sind in den einschlägigen Erlassen definiert (insb. § 16 ff. IDV). Wir empfehlen der JI, betreffend Abläufe und Verantwortlichkeiten **Hilfestellungen** für eine einheitliche und einfache Umsetzung zu

	erarbeiten. Dies umfasst auch das Vorgehen, wenn einem Gesuch nicht entsprochen werden kann. • Es sollte technisch sichergestellt werden, dass die verlangten Daten zeitnahe zusammengestellt werden können. • In der zu erarbeitenden Hilfestellung ist zu beschreiben, wie die Daten der betroffenen Person rechtskonform elektronisch zur Verfügung gestellt werden können. **Gesuche von betroffenen Personen** zum Schutz ihrer Persönlichkeit (§ 21 IDG): • Der **Prozess** zur Bearbeitung von Gesuchen zum Schutz der Persönlichkeit (§ 21 IDG) ergibt sich ebenfalls aus den einschlägigen Erlassen (insb. VRG). Wir empfehlen auch für diese Gesuche, betreffend Abläufen und Verantwortlichkeiten **Hilfestellungen** für eine einheitliche und einfache Umsetzung zu erarbeiten, damit in allen OEs eine zeitnahe Berichtigung, Vernichtung oder Unterlassen der Datenbearbeitung auf Verlangen der betroffenen Person sichergestellt werden kann. • Ebenfalls Teil des Prozesses muss die Prüfung sein, ob die Daten nicht aufgrund gesetzlicher Bestimmungen aufbewahrt werden müssen. • Bzgl. der Vernichtung von elektronischen Personendaten muss zudem definiert werden, wie diese technisch geschehen soll. Im Zusammenhang mit den Gesuchen gemäss § 20 Abs. 1 und § 21 IDG sind die vorhandenen Umsetzungshilfen und Weisungen zu prüfen und gegebenenfalls zu ergänzen bzw. anzupassen. Für alle Bereiche und Systeme, wo im Zusammenhang mit IDG-Gesuchen ein relevantes Risiko für eine Persönlichkeitsverletzung besteht, sollten detaillierte Weisungen erstellt werden. *Empfohlene Umsetzungsebene: Direktion* **Algorithmische Entscheidsysteme / Profiling** Es sind spezifische **Weisungen** zu erstellen für Systeme, die für ein Profiling verwendet werden können. Wir empfehlen diese Weisungen auf kantonaler Ebene zu definieren oder kantonale Vorgaben dazu zu erlassen, sofern diese von mehreren Direktionen zum Einsatz kommen. Dabei ist soweit möglich zu definieren, welche Informationen erfasst werden dürfen und welche nicht (v.a. in Freitextfeldern) und insbesondere, wie die erfassten Informationen verwendet werden dürfen. Werden die Systeme für verschiedene Zwecke eingesetzt, womit auch unterschiedliche Informationen bearbeitet werden müssen, sind entsprechende Weisungen pro Einsatzgebiet zu erstellen. Sofern Profiling in bestimmten Bereichen generell ausgeschlossen werden soll, sind entsprechende Handlungsanweisungen und Kontrollen zu definieren. *Empfohlene Umsetzungsebene: Kanton, bzw. je nach Einsatzbereich* Es sollte geprüft werden, inwiefern das vorgeschriebene **Verzeichnis** der Informationsbestände um ein **Feld** erweitert werden könnte, welches angibt, ob die jeweiligen **Daten für Profiling** verwendet werden dürfen.

	<u>Empfohlene Umsetzungsebene:</u> Kanton Wir empfehlen zudem, einen Prozess zu implementieren, der die **Begrenzung von automatisierten Einzelentscheiden** weiterhin sicherstellt, z.B. im Rahmen des Privacy by Design Prozesses. Um den gesetzlichen Anforderungen zu entsprechen, empfehlen wir in allen Entscheidungsprozessen natürliche **Personen** zu integrieren und/oder zu kontrollieren, ob **in** bestehenden **Entscheidungsprozessen** natürliche Personen eingesetzt sind. *<u>Empfohlene Umsetzungsebene:</u> Kanton* Da Profiling-Daten gemäss IDG als **besondere Personendaten** gelten, empfehlen wir zudem, die damit in Verbindung stehende **Risiken zu analysieren und falls notwendig, zu mitigieren** (z.B. externes Hosting von solchen Tools, Zusammenarbeit mit Dritten, Datensicherheit, etc.). *<u>Empfohlene Umsetzungsebene:</u> Direktion bzw. je nach Einsatzbereich*
Stellungnahme & Massnahmen der JI	Die JI wird die empfohlenen Massnahmen umsetzen und sich – wo sinnvoll und empfohlen – für eine kantonsweite Umsetzung einsetzen. In Bezug auf die **Bearbeitung von Gesuchen** nach § 20 Abs. 2 IDG (Zugang zu den eigenen Personendaten) ist darauf hinzuweisen, dass das Verfahren, die Zuständigkeit (auf Ebene öffentliches Organ) sowie die Form und der Umfang der Auskunftserteilung in der IDV geregelt sind (§§ 16 ff. IDV). Subsidiär kommt das Verwaltungsrechtspflegegesetz (VRG, LS, 175.2) zur Anwendung, auch für Gesuche nach § 21 IDG. Die JI ist bestrebt, soweit möglich und sinnvoll Hilfsmittel für eine einfache und einheitliche Umsetzung der genannten Bestimmungen für die gesamte Direktion zu erarbeiten. Es ist darauf hinzuweisen, dass **automatisierte Einzelentscheidungen** ohne menschliches Zutun unter geltendem Recht nicht zulässig sind und in der JI auch nicht zum Einsatz kommen. Solche würden gemäss einer durch den Kanton Zürich in Auftrag gegebenen Studie zu Künstlicher Intelligenz (Staatskanzlei/Universität Basel, Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen, Schlussbericht vom 28. Februar 2021 zum Vorprojekt IP 6.4, S. 36) Änderungen im Verwaltungsrechtspflegegesetz (VRG, LS 175.2) bedingen, dies insbesondere betreffend Verfahrensgarantien. **Weisungen** für Systeme, die für ein Profiling verwendet werden können, machen nur je Einsatzgebiet Sinn und können nicht gesamtkantonal geregelt werden. Bezüglich der Empfehlung zur **Ergänzung des Verzeichnisses über die Informationsbestände um Angaben über das „Profiling“** verweisen wir zunächst auf unsere Stellungnahme unter Ziff. 2.1. Zudem ist darauf hinzuweisen, dass gemäss Entwurf des Regierungsrates zum totalrevidierten IDG die öffentlichen Organe künftig ein Verzeichnis über algorithmische Entscheidsysteme (AES) führen müssen, die sich auf die Grundrechte auswirken können. Der Regierungsrat wird die Einzelheiten auf Verordnungsstufe regeln (§ 13 Abs. 3 E-IDG). Dabei werden das Verzeichnis über die Informationsbestände, der (neu einzuführende) Datenkatalog sowie das Verzeichnis über die algorithmischen

	Entscheidsysteme zusammen angedacht und konkretisiert werden müssen. Zum Verzeichnis über die Informationsbestände verweisen wir auf unsere Stellungnahme zu Ziff. 2.1.

2.10 Schulungen & Sensibilisierung

Feststellungen	Die befragten Personen verfügten – je nach Bereich – über unterschiedliches Datenschutzwissen. Bei den nach GOG- und StJVG-Vorgaben benannten Datenschutzberatenden in der OSTA, OJUGA und JuWe., die gleichzeitig auch die D&I-Verantwortlichen ihrer OE sind, ist dieses Wissen ausgeprägt. Weitere Ansprechpersonen hatten bereits Datenschutzweiterbildungen absolviert (z.B. JuWe-AL, HRA). Jedoch gibt es auch unter den gemäss JIOV nominierten D&I-Verantwortlichen Personen, für die das Thema neu ist. Dies betrifft die kleinen Fachstellen, die mit wenigen sowie weniger sensiblen Personendaten arbeiten und in juristischen Belangen vom GS SRD unterstützt werden (z.B. FK, FI). Für die Mitarbeitenden des JuWe werden im Rahmen der JuWe-Akademie bereits 4x pro Jahr freiwillige Datenschutz-Schulungen angeboten. Diese sind allerdings nur im BVD obligatorisch, wo mit besonders sensiblen Daten gearbeitet wird. Ansonsten werden die Mitarbeitenden bei den meisten Organisationseinheiten beim Eintritt im Zusammenhang mit den Amtsgeheimnis-Vorschriften für den Datenschutz sensibilisiert. Refresher-Kurse werden jedoch keine durchgeführt. Sensibilisierungen zu bestimmten Themen (z.B. Home Office Regeln während der Pandemie) werden informell im Rahmen von Teamsitzungen gemacht. Das JuWe informiert zudem im «JuWe aktuell»-Newsletter zu Datenschutz-Thematiken. Für das Thema der Informationssicherheit gibt es bei DigiSol ein Projekt für ein E-Learning, das die JI zusammen mit der Bildungsdirektion realisiert (Lucy). So sollen demnächst zwei Module im "Kompent» released werden. Der Release war zum Zeitpunkt der Vertiefungsinterviews für Ende Q2 geplant. Ebenso besteht eine DigiSol-Intranetseite mit Informationen zu Phishing-Kampagnen und ein DigiSol-Newsletterversand. Regelmässige Datenschutz- und Informationssicherheitsschulungen für sämtliche JI-Mitarbeitende gibt es nicht.
Empfehlungen	Das Thema «Datenschutz-Bewusstsein» sollte auf kantonaler Ebene angegangen werden. Generell müsste das Bewusstsein für das Thema Datenschutz nicht nur im Rahmen der amts- und fachstellenspezifischen Schulungen beim Eintritt geschaffen, sondern durch **regelmässige, obligatorische Schulungen und Refresher-Kurse für alle Mitarbeitenden (z.B. eLearnings) sichergestellt werden.** Diesbezüglich empfehlen wir, bereits bestehende Schulungsmaterialien (z.B. der JuWe-Akademie) zu sichten und diese ggf. auch den anderen

	Organisationseinheiten verfügbar zu machen. Wir empfehlen diese Massnahmen kantonal einheitlich zu gestalten. *Empfohlene Umsetzungsebene: Kanton*

Stellungnahme & Massnahmen der JI	Die Notwendigkeit flächendeckender und **regelmässiger Schulung und Sensibilisierung** der Mitarbeitenden zum Thema D&I wurde in der JI erkannt. Die JI wird die empfohlenen Massnahmen umsetzen und sich für ein gesamtkantonales Curriculum für alle Mitarbeitenden des Kantons einsetzen. Die Schulung und Sensibilisierung sollen auch im Rahmen der initiierten **Compliance-Organisation D&I@JI** einen hohen Stellenwert erhalten. In einem ersten Schritt sollen die D&I-Verantwortlichen als Schlüsselpersonen in ihren Einheiten weiter geschult und durch das GS inhaltlich besonders unterstützt werden (vgl. Stellungnahme zu Ziff. 2.1). Ab 2024 wird das Thema Informationssicherheit Teil der JuWe Academy sein (Termine stehen fest). Der durchgeführte **Awareness Pilot** mit den Modulen von Lucy (im Q1 2023), wurde überarbeitet und erweitert: ein IS-Einstiegsmodul und 6 weitere Module wurden zusammengestellt und sind Teil der Pflichtschulung. Die Kurseinladung wurde anfangs Dezember 2023 verschickt und ist für alle JI-Mitarbeitende obligatorisch. Es wird zurzeit ein **Awareness-Programm für das Jahr 2024** zusammengestellt. E-Learnings stehen in Zusammenarbeit mit dem Competence Center Cyber Security für die JI zur Verfügung ebenso Präsentationen (online) zum Umgang mit Speichermedien und Daten. Neu werden im JuWe Plakate und Postkarten in den Kaffeeräumen verteilt, um auch weitere Mitarbeitende zu erreichen, welche kein persönliches Notebook besitzen. Allgemein versuchen wir vor allem das Thema „Phishing“ anzugehen. Schliesslich wird der **Roll out des DAP** zum Anlass für eine Informations- und Sensibilisierungsoffensive in der ganzen JI genutzt. Das **Staatsarchiv** spricht in seiner täglichen Arbeit mit den anbietepflichtigen Stellen Informationssicherheits- und Datenschutzfragen regelmässig an und macht Vorschläge für die konkrete und angemessene Umsetzung solcher Regeln pro Amt. **Anknüpfend an aktuelle Gesetzesänderungen** wie das Inkrafttreten von Digilex, die Revision des IDG, etc. soll in Zusammenarbeit mit der Kommunikationsabteilung der JI ein entsprechendes Schulungs- und Kommunikationskonzept erstellt werden. So sollen die in den OEs stattfindenden Massnahmen besser koordiniert und genutzt werden.

2.11 Verletzung der Datensicherheit

Feststellungen	Wird eine potenzielle Verletzung der Datensicherheit von der IT festgestellt, führen in einem ersten Schritt das AFI (Endpoints) oder die DigiSol (eigene Infrastruktur) eine technische Untersuchung durch. Je nachdem, wo die Verletzung vermutet wird, untersuchen das AFI oder die DigiSol den Vorfall (sog. «Incident»). Zudem beruft die DigiSol ein Ad-hoc-Gremium zur Abstimmung mit dem AFI (ISIK, ISIDs, Leitende IT) ein. Wird ein solcher Incident bei einer Organisationseinheit entdeckt, bearbeitet diese den Fall alsdann individuell. Der Vorfall muss den Vorgesetzten gemeldet werden. Ein formeller Prozess für die Bearbeitung und Meldung von Verletzungen der Datensicherheit, der dem «State-of-the-Art» für vergleichbare Organisationen entspricht, fehlt. Ebenso besteht bei der JI kein Notfallplan zur Behebung von Datensicherheitsverletzungen (sog. «Breach Response Plan»). Wie der GS-SRD als Kompetenzzentrum für den Datenschutz in einem Datenschutzvorfall integriert würde, ist nicht klar geregelt.
Empfehlungen	Die Verfahren bei einer Datenschutzverletzung sollten auf kantonaler Ebene festgelegt und umgesetzt werden. Die JI muss einen entsprechenden **formellen Prozess** mit klar zugewiesenen **Verantwortlichkeiten** und Ansprechpartnern definieren, um Datensicherheitsverletzungsmeldungen effizient und im Rahmen der Anforderungen der (revidierten) IDG-Gesetzgebung zu behandeln. Wir empfehlen, mit Templates und Checklisten das **Vorfall-Management** (Incident Management) und die allfälligen Notifikationen effizienter zu gestalten und den Prozess mit den jeweiligen Ansprechpersonen intern angemessen zu kommunizieren (z.B. via Intranet oder Richtlinien). Zudem sollten, soweit möglich, bereits jetzt **angemessene Notfallpläne mit Sofortmassnahmen** (z.B. sofortiger Stopp der Datenbearbeitung, Entzug von Zugriffsrechten etc.) sowie Massnahmen zur Schadensminderung und Prävention für denkbare Fälle von Datensicherheitsverletzungen evaluiert werden. *Empfohlene Umsetzungsebene: Kanton*
Stellungnahme & Massnahmen der JI	Ein umfangreicher Incident Prozess fehlt zurzeit und wird als Massnahme von der Finanzdirektion erstellt. In der Zwischenzeit wurde im Intranet für die gesamte kantonale Verwaltung eine Handlungsanleitung mit Kontaktdaten aufgeschaltet (Vorfall melden; https://sicher.ktzh.ch/intranet/informationssicherheit/de/vorfall-melden.html).

3 Aktionsplan

Gestützt auf die Erhebung schlägt die KPMG den folgenden Aktionsplan vor und definiert die Umsetzungsvoraussetzungen. Ferner umreisst die KPMG, welche Voraussetzungen geschaffen werden müssen, um die Vorhaben weiter vorantreiben zu können.

3.1 Plan

Wir empfehlen der JI, gestützt auf die obigen Empfehlungen einen Aktionsplan auszuarbeiten. Dieser hängt massgeblich von der Governance und den Entscheiden (vgl. Ziff. 4.3) sowie den zur Verfügung stehenden Ressourcen (vgl. Ziff. 4.4) ab.

Aus obigen Empfehlungen ergeben sich sowohl sogenannte „Quick Wins“ (relativ kurzfristig und schnell umsetzbare Massnahmen), als auch längerfristige Massnahmen (mit grösserem Aufwand umsetzbar). Wir empfehlen der JI die folgende Priorisierung der Quick Wins und längerfristigen Massnahmen.

3.1.1 Massnahmen: Priorisierung der Quick Wins

Die KPMG empfiehlt die folgenden Quick-Win-Massnahmen zur Umsetzung. Diese können direkt auf Ebene Direktion speditiv umgesetzt werden:

1. **Zuständigkeiten:** Die Verantwortlichkeiten und Zuständigkeiten für D&I und die damit einhergehenden Aufgaben in den Fachstellen und Ämtern müssen weiter definiert werden (Rollen- und Aufgabenklärung D&I-Verantwortliche auf Stufe GS und OE).
2. **Schulung / Sensibilisierung:** Es sind entsprechende D&I Schulungs- und Sensibilisierungsmassnahmen zu definieren und durchzuführen.
3. **Verzeichnis der Informationsbestände:** Die Verzeichnisse der Informationsbestände sind gemäss aktuellem Bestand der Datenverwaltungssysteme zu aktualisieren und/oder neu zu erstellen.
4. **Überprüfen der Einwilligungen:** Datenbearbeitungen basierend auf Einwilligungen sind daraufhin zu überprüfen, ob sie gemäss Spezialgesetzen oder § 9 IDG zulässig sind.
5. **Drittparteienmanagement:** Verträge mit Dritten sind daraufhin zu überprüfen, ob diese die notwendigen standardvertraglichen Regelungen und Geheimhaltungserklärungen gemäss DSB-Vorgaben beinhalten.
6. **Datensicherheitsverletzungen:** Es sind Vorgaben und ein entsprechender Prozess für das Vorgehen bei Datensicherheitsverletzungen zu definieren und umzusetzen.

3.1.2 Massnahmen: Priorisierung längerfristiger Massnahmen

Die KPMG empfiehlt die folgenden längerfristigen Massnahmen zur Umsetzung. Optimalerweise werden diese auf **kantonaler Ebene** vorgegeben, oder es werden kantonale Vorgaben zu deren Definition und Umsetzung definiert:

1. **Datenschutz,-Risk-&-Compliance- Rahmenwerk:** Die operative Durchführung der D&I Aufgaben in den Fachstellen und Ämtern und deren regelmässige Überprüfung müssen definiert und umgesetzt werden. Die Definition eines Datenschutz-, Risk-&-Compliance-Rahmenwerks (nachfolgend: Rahmenwerk) soll es Mitarbeitenden ermöglichen, unter Einbezug der relevanten Gesetze die Compliance-Vorschriften

einzuhalten. Das Rahmenwerk bietet eine praktische und pragmatische Struktur, um den täglichen Betrieb der Organisation professionell zu managen und Datenschutzrisiken zu minimieren.

2. **Privacy by Design & Default:** Für Änderungen und Neuimplementierungen ist ein „Privacy by Design & Default"-Prozess zu definieren und zu implementieren, welcher die Datenschutzaspekte zwingend berücksichtigt.

3. **Datenschutz-Policy:** Erarbeitung und Kommunikation einer für alle einfach verständlichen, das Wesentliche regelnden Datenschutz-Policy für alle Mitarbeitenden. Darüber hinaus bereitstellen und aktuell halten einer zentralen Sammlung sämtlicher relevanter Datenschutzgrundlagen, auf welche jederzeit und mit einfachen Suchbegriffen zugegriffen werden kann.

4. **Datenmanagement:** Zur Sicherstellung der Qualität, der rechtmässigen Aufbewahrung und anschliessenden Archivierung oder Vernichtung der Personendaten sind entsprechende zusätzliche Massnahmen zu implementieren. Dies kann insbesondere mit der Einführung von Purview unterstützt werden.

5. **Sicherheitsmassnahmen:** Sicherheitsmassnahmen wie Identity Management, Berechtigungskonzepte oder Verschlüsselung bei Datenhaltung und Datentransfers sind zu überprüfen und hinlänglich umzusetzen.

6. **Drittparteienmanagement:** Direktionsweite Vorgaben für technische und organisatorische Massnahmen, regelmässige Lieferantenaudits und ggf. erforderliche Zertifizierungen sind zu definieren.

3.2 Umsetzungsvoraussetzungen

Seitens KPMG sei hier nochmals mit Nachdruck darauf hingewiesen, dass es sich beim Datenschutz und der Informationssicherheit um ein alle Bereiche der kantonalen Verwaltung durchdringendes Grossprojekt handelt, welches vielerorts eine neue Bewusstseinsbildung sowie eine dauerhafte Änderung der bisherigen Verfahren und Verhaltensweisen erfordert.

Dieses Projekt ist auf allen Ebenen anspruchsvoll: technisch, organisatorisch wie auch juristisch. Letztere drei Elemente müssen so orchestriert werden, dass sie im optimalen Zusammenspiel einen der aktuellen Bedrohungslage angemessenen Schutz zu vertretbaren Kosten gewährleisten. Dies ist angesichts des technischen Fortschritts und der neu entstehenden gesetzlichen Grundlagen eine dauerhafte Herausforderung!

Ein solches Veränderungsprojekt kann daher nur durch starken Support und Involvement der Obersten Führung, durch Know-how Aufbau und unter Einsatz hinlänglicher Ressourcen sowie auf Basis eines langfristigen, risikobasierten und nach Prioritäten ausgerichteten, immer wieder nachjustierten Plan gelingen.

Es gibt also eine Reihe von Voraussetzungen, welche für eine effektive Umsetzung der Massnahmen berücksichtigt werden müssen. Insbesondere sind dies die Governance, die flächendeckende Bewusstseinsbildung für den Datenschutz und die Informationssicherheit, die mit den verfügbaren Ressourcen stemmbaren Vorhaben, die Nutzung von Synergien und Unterstützungsmöglichkeiten, die Gewährleistung der Umsetzungssicherheit durch Definition von Rollen und Verantwortlichkeiten, griffige Kontrollmechanismen sowie die Schaffung der notwendigen Rahmenbedingungen.

Um im Projekt effizient zu sein, sind Kreativität sowie die Nutzung aller möglicher Synergiepotentiale gefragt. Es gibt eine Reihe von gleichen Massnahmen, welche an

verschiedenen Stellen umgesetzt werden müssen. Die Ressourcen hierfür sind knapp. Hier gilt es, durch kluges Design maximale Synergien zu schöpfen und grösstmögliche zentrale Unterstützung bereitzustellen (z.B. mittels Repositories, d.h. zentralen Ablagen für Dokumente, welche allen dienlich sind).

Das Zuteilen der Umsetzungsmassnahmen ist das Einfachste. Das Schwierigste ist deren Umsetzung – nicht einmalig, sondern laufend. Hierzu braucht es hinlängliche Ressourcen, klar definierte und allozierte Rollen und Verantwortlichkeiten sowie Kontrollmechanismen. All dies sollte von Beginn weg mitgegeben werden, um die Umsetzung fortlaufend sicherzustellen.

3.3 Governance & Entscheide

Um das weitere Vorgehen managen zu können, bedarf es in erster Linie der Governance der Führungsebene, bestehend aus den kantonalen und den direktionalen Verantwortlichen.

Da der Datenschutz alle Bereiche durchdringt, ist darunter bis auf Ebene der verantwortlichen Mitarbeitenden (z.B. Data Owners) die Governance sowie die personalrechtlich untermauerte Zuständigkeit und Weisungsbefugnis auszudehnen.

Da die in der Governance verantwortlichen Führungskräfte risikobasierte Entscheide fällen können müssen, ist zu Beginn sicherzustellen, dass die sehr anspruchsvolle Fachkompetenz, welche je in den Bereichen Technik, Organisation und Recht gefordert ist, weiter aufgebaut wird und sich alle darüber einig sind, wie der risikobasierte Ansatz gefahren werden und wie die Entscheidungsfindung stattfinden soll.

Diese Governance ist ganz zu Beginn des Datenschutzumsetzungsprojekts zu konstituieren inkl. der Klärung der Rollen und Verantwortlichkeiten für die jeweiligen Themen. Zudem muss deren Entscheidungskompetenz, Weisungsbefugnis sowie das verfügbare Budget und die Budgetkompetenz pro Rolle festgelegt werden.

Es stehen daher folgende Entscheide an:

- Wer trägt die Verantwortung für alles, was den gesamten Kanton anbelangt?
- Wie sollen Entscheide gefällt werden? Wer soll diese fällen?
- Wie sollen die Ressourcen beantragt werden?
- Wer hat für was die Budgetkompetenz? Wer steuert das Budget?
- Wie und nach welchen Kriterien werden Risiken eruiert und risikobasierte Entscheide getroffen?
- Wie viele Ressourcen müssen in dieses Vorhaben eingebracht werden? Woher kommen diese und wer ist wie über diese Ressourcen weisungsbefugt?
- Soll über die kantonale Verwaltung hinweg ein einheitliches Datenschutz-, Informationssicherheits-, Risk- & Compliance-Regelwerk aufgezogen werden mit entsprechenden Kontrollmechanismen und Verantwortlichen, welche nach den Projektarbeiten das Hochhalten des Datenschutzes sicherstellen?

Ohne das Fällen dieser Entscheide kann das Datenschutzvorhaben im Anschluss nicht umgesetzt werden, ohne dass es zu grösseren Verzögerungen oder gar zum Stillstand kommt, weil unterwegs politische oder Ressourcen-Fragen gelöst werden müssen. Solche

Verzögerungen würden denn auch zwangsläufig zu vermeidbaren, erheblich höheren Kosten führen.

3.4 Ressourcenbedarf

Der erforderliche Ressourcenbedarf ist abhängig von:

- dem angestrebten Umfang des Datenschutz-, Risk- & Compliance-Regelwerks (kantonal, direktional oder auf Stufe Organisationseinheit)
- den risikobasiert zu treffenden Massnahmen
- den betroffenen Systemen und deren Änderungsbedarf
- dem Verhältnis externe vs. interne Ressourcen und deren Verfügbarkeit
- der Staffelung und Dauer des Vorhabens
- der Komplexität der angestrebten Massnahmen
- dem Grad der Standardisierung und Automatisierung, der gewählt wird

Entsprechend ist das Vorhaben als Ganzes zu Beginn im Groben zu planen und abzustimmen, bevor man eine Aussage zu den Ressourcen machen kann. Die Aufwandschätzung der einzelnen Aktivitäten erlaubt es denn auch, nochmals risiko- und kostenbasiert festzulegen, welcher Mittel- und Ressourcenbedarf effektiv erforderlich und angemessen sein wird.

Ende des KPMG Berichts

4 Weiteres Vorgehen

4.1 Laufende Umsetzung der Massnahmen gemäss Aktionsplan

Die Umsetzung der Massnahmen gemäss Aktionsplan erfolgte soweit möglich bereits während der Erhebungen, oder wurde initiiert. Insbesondere wurden Massnahmen an die Hand genommen, die innerhalb der bestehenden Strukturen, Zuständigkeiten und Abläufen realisiert werden können. Hierbei stehen insbesondere Quick Wins im Vordergrund.

Beispiele hierfür sind die Einsetzung der D&I-Verantwortlichen, die Lancierung einer Intranetseite sowie Awareness – Schulungen, Aktualisierung der Informationsbeständeverzeichnisse und insbesondere die Prozessdefinition betr. Datenschutz für den Vertragsabschluss mit Dritten.

4.2 Aufbau eines Compliance Management – System im Bereich D&I

Aufgrund der Empfehlungen der KPMG zur Schaffung eines «Datenschutz- Risk-&-Compliance-Rahmenwerk» soll für die Umsetzung und die nachhaltige Implementierung der langfristigen Massnahmen ein Compliance - Management - System (CMS) innerhalb der JI aufgebaut werden. Hierbei gilt es, an den bestehenden Ressourcen anzuknüpfen. Erste Schritte wurden bereits unternommen, z.B. durch Schaffung des Fachbereichs Infodat auf Direktionsebene, oder die Bestimmung von D&I-Verantwortlichen in den Organisationseinheiten. Seitens KPMG wird darauf hingewiesen, dass für den Aufbau eines CMS zusätzlichen Ressourcen notwendig sind, einerseits um die Strukturen und Prozesse aufzubauen, andererseits um den Datenschutz und die Informationssicherheit auch langfristig gewährleisten zu können.

Weiter empfiehlt KPMG der JI den Einsatz eines elektronischen Governance, Risk und Compliance Systems (eGRC). Dieses hilft im Sinne der «Lean Compliance», zentrale Ablagen z.B. für Policies bereitzustellen und den Mitarbeitenden bekannt zu machen, die Governance aktuell zu halten (z.B. automatisches Melden bei Stellenwechseln von Verantwortlichen Personen) Compliance Prozesse und Aufgaben vollständig zu automatisieren und vor allem mittels Kontrollmechanismen deren Durchführung kontinuierlich sicherzustellen und zu dokumentieren. Damit können im ganzen Kanton substanziell Compliance Kosten eingespart sowie die Effektivität und die Umsetzungsgeschwindigkeit der anberaumten Datenschutzmassnahmen erhöht werden.

Schliesslich empfiehlt KPMG, alle D&I Funktionalitäten, die im Microsoft Office 365 E5 bereitgestellt werden, von Beginn weg zu konfigurieren und konsequent zu nutzen. Damit können Massnahmen wie Identifikationsverfahren, Zugriffsrechte, Datenkategorisierungen, Betroffenenrechte etc. im Sinne von Privacy by Design & Default rasch und wirksam umgesetzt werden.

4.3 Direktionsübergreifende Kooperation

Mit Blick auf Massnahmen, die sinnvollerweise gesamtkantonal einheitlich organisiert werden sollten, ist geplant, die Zusammenarbeit mit den anderen Akteuren, namentlich dem Amt für Informatik, welches für die Grundversorgung im Bereich IKT sowie die Cybersicherheit zuständig ist, der Compliance – Beauftragten im Bereich Schulung und Sensibilisierungsmassnahmen, sowie den anderen Direktionen zu intensivieren. Dies betrifft z.B. die Definition von Prozessen bei Datensicherheitsverletzungen, oder technische Massnahmen zu «Privacy by Design & Default» sowie die Konzeption von Awareness-Kampagnen oder Schulungen im Bereich D&I.

5 Anhänge

Abkürzungsverzeichnis

Abkürzung	Vollständige Bezeichnung
AFI	Amt für Informatik
BCM	Business Continuity Management
BR	Bezirksrat
BRK	Bezirksratskanzlei
BVD	Bewährungs- und Vollzugsdienste
DigiSol	Digital Solutions
D&I@JI	D&I in der Direktion der Justiz und des Innern
D&I	D&I
D&I-Verantwortliche/r	Verantwortlicher für die Einhaltung der Vorschriften des Datenschutz und der Informationssicherheit
DSG	Revidiertes Bundesgesetz über den Datenschutz
DSFA	Datenschutz-Folgenabschätzung
F&E	Forschung und Entwicklung
FG	Fachstelle Gleichstellung
FI	Fachstelle Integration
FK	Fachstelle Kultur
FOTRES	Forensisches Operationalisiertes Therapie-Risiko-Evaluations-System
GAZ	Gemeindeamt
GOG	Gesetz über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess (GOG)
GS	Generalsekretariat
Komm	Kommunikation
HR	Human Resources (Personalabteilung)
HRA	Handelsregisteramt
IDG	Gesetz über die Information und den Datenschutz (IDG)
IT	Informatik

ISO	Internationale Organisation für Normung
ISAE	International Standard on Assurance Engagements
ISID	Informationssicherheitsbeauftragter der Direktion
ISIK	Informationssicherheitskommission des Kantons
JI	Direktion der Justiz und des Innern
JIOV	Organisationsverordnung der Direktion der Justiz und des Innern (JIOV)
JSP	Jugendstrafrechtspflege
JUGA	Jugendanwaltschaft
JuWe	Justizvollzug und Wiedereingliederung
JVA	Justizvollzugsanstalt
KOH	Kantonale Opferhilfestelle
MZU	Massnahmenzentrum Uitikon
OJUGA	Oberjugendanwaltschaft
OSTA	Oberstaatsanwaltschaft
PPD	Psychiatrisch-Psychologischer Dienst
PR-Agentur	Public Relations-Agentur
RIS	Rechtsinformationssystem
ROS	Risikoorientierter Sanktionenvollzug
SHA	Statthalteramt
SRD	Stabs- und Rechtsdienst
STA	Staatsanwaltschaft
STAT	Statistisches Amt
StAZH	Staatsarchiv
UGZ	Untersuchungsgefängnisse Zürich
VEZ	Vollzugseinrichtungen Zürich