Stadt Kloten **2022-01**

Datenschutzreglement

Vom 24. Mai 2022

Von diesem Geschäft tangierte Erlasse (SRS Nummern)

Neu:	**1.2-2**
Geändert:	–
Aufgehoben:	1.2-2

Der Stadtrat,

gestützt auf Art. 27 der Gemeindeordnung (GO; SRS 1.1-1) und in Anwendung von §13 des Gesetzes über die Information und den Datenschutz (IDG; LS 170.4),

beschliesst:

I.

Art. 1 Zweck und Grundlagen

[1] Dieses Datenschutzreglement enthält Vorschriften zum Schutz von Personendaten, die für alle Mitarbeitenden der Behörden und Dienststellen der Stadt Kloten gelten. Es legt die Bedeutung und den Stellenwert des Datenschutzes im Sinne der Achtung der Grundrechte und Grundfreiheiten der Mitarbeitenden, der betroffenen Bevölkerung und der Geschäftspartner fest.

[2] Als Grundlage für das Datenschutzreglement dient das Gesetz über die Information und den Datenschutz des Kantons Zürich (IDG) und die dazugehörige Verordnung über die Information und den Datenschutz des Kantons Zürich (IDV). Soweit anwendbar, beruht sie ebenfalls auf dem revidierten Bundesgesetz über den Datenschutz (DSG) sowie der revidierten Verordnung zum Bundesgesetz über den Datenschutz (VDSG). Das vorliegende Reglement nimmt die Vorgaben aus den gesetzlichen Grundlagen auf und konkretisiert diese für die Mitarbeitenden der Behörden und Dienststellen der Stadt Kloten.

Art. 2 Darum geht es

[1] Das Datenschutzreglement regelt die Bearbeitung von Personendaten:

a. Personendaten sind alle Daten, die sich auf eine natürliche Person beziehen.

b. Bearbeitung bedeutet Erheben, Ordnen, Speichern, Verändern, Offenlegen, Übermitteln, Einschränkung, Löschen oder Vernichten von Daten. Das gilt für physische oder elektronische Daten.

c. Besondere Personendaten sind (gemäss IDG § 3 Abs. 4):
   1. Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht, wie Informationen über
   1.1 die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
   1.2 die Gesundheit, die Intimsphäre, die ethnische Herkunft sowie genetische und biometrische Daten,
   1.3 Massnahmen der sozialen Hilfe,
   1.4 administrative oder strafrechtliche Verfolgungen oder Sanktionen.
   2. Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben (Persönlichkeitsprofil),
   3. automatisierte Auswertungen von Informationen, um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen (Profiling).

Art. 3 Grundsätze für die Bearbeitung

[1] Bei der Bearbeitung von Personendaten sind insbesondere folgende Grundsätze des IDG einzuhalten:

a. Gesetzmässigkeit (§ 8 IDG):
   1. Personendaten dürfen bearbeitet werden, soweit dies zur Erfüllung der gesetzlich umschriebenen Aufgaben der Stadt Kloten geeignet und erforderlich ist.
   2. Besondere Personendaten werden nur bearbeitet, wenn dafür eine hinreichende Bestimmung in einem formellen Gesetz besteht.

b. Verhältnismässigkeit (§ 8 Abs. 1 IDG): Personendaten dürfen nur so weit bearbeitet werden, als dies für die Aufgabenerfüllung geeignet und erforderlich ist.

c. Transparenz (§ 4 IDG): Der Umgang mit Personendaten ist so zu gestalten, damit rasch, umfassend und sachlich informiert werden kann.

d. Zweckbindung (§ 9 IDG): Personendaten dürfen nur zu dem Zweck bearbeitet werden, für den sie erhoben worden sind. Eine Ausnahme besteht dann, wenn eine rechtliche Bestimmung eine weitere Bearbeitung erlaubt, oder wenn die betroffene Person im Einzelfall eingewilligt hat. Anonymisierte Daten können im Rahmen von Statistiken bearbeitet werden.

r. Vermeidung des Personenbezugs (§ 11 IDG): Datenbearbeitungssysteme und -programme sind so zu gestalten, dass möglichst nur Personendaten anfallen, die zur Aufgabenerfüllung notwendig sind. Soweit möglich sind Personendaten zu löschen, anonymisieren oder pseudonymisieren. Anonymisierte Daten dürfen ohne Einschränkung bearbeitet werden, solange keine Rückschlüsse auf die betroffenen Personen möglich sind.

Art. 4 Rechte der betroffenen Personen

[1] Zu beachten sind die Rechte der betroffenen Personen nach IDG:

a. Informationspflicht bei Erhebung von Personendaten (§ 12 IDG): Die betroffenen Personen sind über Zweck und Rahmenbedingungen der Erhebung und über ihre Rechte zu informieren.

b. Auskunftsrecht (§ 20 IDG): Jede betroffene Person kann eine Bestätigung darüber verlangen, ob sie betreffende Personendaten bearbeitet werden.

c. Recht auf Berichtigung (§ 21 IDG): Die betroffene Person kann die Berichtigung oder Vernichtung sie betreffender unrichtiger Personendaten verlangen.

d. Widerrechtlichkeit des Bearbeitens (§ 21 IDG): Die betroffene Person kann die Widerrechtlichkeit der Bearbeitung feststellen lassen sowie verlangen, dass die Folgen des widerrechtlichen Bearbeitens beseitigt werden.

e. Recht auf Datensperrung (§ 22 IDG):
   1. Wenn die Stadt Kloten Personendaten an Private bekanntgibt, kann die betroffene Person diese Bekanntgabe sperren lassen. Personendaten dürfen an Gesuchstellende dennoch bekannt gegeben werden, wenn diese nachweisen kann, dass die Sperrung sie an der Verfolgung eigener Rechte gegenüber der betroffenen Person hindert.
   2. Im Zweifelsfalle ist stets vorgängig die Datenschutzorganisation (bestehend aus Datenschutzkoordinator und dem externen Datenschutzbeauftragten der Stadt Kloten) zu kontaktieren.

Art. 5 Verzeichnis der Informationsbestände (§ 14 Abs. 4 IDG)

[1] Ein Verzeichnis der Informationsbestände ist zu führen. Dieses beinhaltet insbesondere die Zwecke der Bearbeitung und eine Kennzeichnung von Informationsbeständen, welche Personendaten beinhalten. Es ist öffentlich zugänglich.

Art. 6 Klassifizierung der Personendaten (§ 7 Abs. 2 IDG)

[1] Personendaten sind wie folgt zu klassifizieren:

a. Keine Personendaten (D0):
   1. Darunter fallen Informationen, die keine Angaben zu bestimmten oder bestimmbaren natürlichen Personen enthalten.
   2. Beispiel: Angaben über Branchen-Durchschnittslöhne.

b. (Nicht-sensible) Personendaten (geringes bis mittleres Risiko, D1):
   1. Personendaten, welche keine besondere Schutzwürdigkeit aufweisen, mitunter nicht unter die nachfolgenden Kategorien D2 oder D3 fallen.
   2. Beispiel: (1) Liste mit den E-Mail-Adressen der Newsletterempfänger; (2) (in der Regel) die private Adresse der Mitarbeitenden.

c. Besondere Personendaten (hohes Risiko, D2):
   1. Darunter fallen Informationen, die besondere Personendaten enthalten.
   2. Beispiel: Arztzeugnisse.

d. Hochsensible Personendaten (sehr hohes Risiko, D3):
   1. Personendaten, deren Missbrauch für den Betroffenen Gefahren für Gesundheit und Leben bedeuten. Wenn das Bekanntwerden von besonderen Personendaten zur Bedrohung, insbesondere an Leib und Leben der betroffenen Person führen kann, dann spricht man von hochsensiblen (lebenswichtigen) Personendaten.
   2. Beispiel: Personalien von Bewohnerinnen eines Frauenhauses.

[2] Dateneigner klassifizieren die ihnen zugeordneten Datenbestände. Diese Klassifizierung wird zudem von der Datenschutzorganisation in das Verzeichnis der Informationsbestände aufgenommen.

[3] Sind besondere oder hochsensible Personendaten betroffen, so ist der Datenschutzbeauftragte zu informieren.

Art. 7 Übermittlung von Daten an Dritte

[1] Bearbeitung im Auftrag (§ 6 IDG): Datenbearbeitungen können an Dritte übertragen werden, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung dem entgegensteht. Bevor eine Datenbearbeitung an Dritte übertragen wird, ist die Datenschutzorganisation der Stadt Kloten zu kontaktieren.

[2] Bekanntgabe von Personendaten (§ 16 ff. IDG): Bevor Personendaten an Dritte bekanntgegeben werden, ist die Datenschutzorganisation der Stadt Kloten zu informieren. Grundsätzlich gelten die Vorschriften von § 16 – 19 IDG für die Weitergabe von Personendaten an Dritte. Dabei dürfen Personendaten nur dann bekanntgegeben werden, wenn eine rechtliche Bestimmung dazu ermächtigt (Fürsorgepflichten, Anzeigepflichten etc.), die betroffene Person eingewilligt hat, es zur Abwendung einer unmittelbar drohenden Gefahr für Leib und Leben unentbehrlich oder der notwendige Schutz anderer wesentlicher Rechtsgüter höher zu gewichten ist oder ein anderes öffentliches Organ die Personendaten im Einzelfall zur Erfüllung seiner gesetzlichen Aufgabe benötigt (Amtshilfe). Für die Bekanntgabe besonderer Personendaten ist eine hinreichend bestimmte Regelung in einem formellen Gesetz erforderlich (§ 17 IDG). Des Weiteren dürfen der Datenbekanntgabe keine rechtliche Bestimmung oder überwiegende öffentliche oder private Interessen entgegenstehen (§ 23 IDG).

[3] Bekanntgabe für nicht personenbezogene Zwecke: Personendaten dürfen zur Bearbeitung für nicht personenbezogene Zwecke, z.B. Forschung, Statistik oder Planung bekanntgegeben werden. Der jeweilige Empfänger hat nachzuweisen, dass die Personendaten anonymisiert werden, aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind und die ursprünglichen Personendaten nach der Auswertung vernichtet werden.

[4] Amtsgeheimnis: Liegt eine gesetzliche Grundlage zur Datenbekanntgabe vor, ist keine formelle behördliche Entbindung von der Schweigepflicht im Sinne von Art. 320 Ziff. 2 Strafgesetzbuch (StGB) notwendig. Im Zweifelsfalle entscheidet die Datenschutzorganisation der Stadt Kloten über die Notwendigkeit der formellen behördlichen Entbindung.

[5] Spezialgesetze: Für die einzelnen Verwaltungseinheiten gelten zudem die Bestimmungen der jeweils einschlägigen Spezialgesetze (wie die Zivilstandsverordnungen des Bundes und des Kantons oder das kantonale Gesetz über das Meldewesen und die Einwohnerregister).

Art. 8 Technische und organisatorische Massnahmen (§ 7 IDG)

[1] Die Stadt Kloten trifft angemessene technische und organisatorische Massnahmen, um das vorliegende Datenschutzreglement wirksam umzusetzen und die Sicherheit der Personendaten zu gewährleisten.

[2] Die zu bearbeitenden Personendaten werden vom zuständigen Dateneigner gemäss Kapitel 6 klassifiziert. Basierend auf ihrer Klassifizierung sind die Personendaten mit entsprechend geeigneten technischen und organisatorischen Massnahmen zu schützen.

Art. 9 Datenschutz-Folgenabschätzung (§ 10 IDG)

[1] Ist eine neue Bearbeitungstätigkeit von Personendaten geplant, sind die Risiken für die Grundrechte der betroffenen Personen zu bewerten. Dafür ist der Datenschutzkoordinator der Stadt Kloten zu kontaktieren. Dieser zieht bei besonderen Risiken den externen Datenschutzbeauftragten und/oder den kantonalen Datenschutzbeauftragten bei.

Art. 10 Meldung von Vorfällen (§ 12a IDG)

[1] Wird eine Verletzung des Schutzes von Personendaten erkannt oder vermutet, ist dies unverzüglich via Service Request im Self Service Portal) zu erfassen oder via E-Mail oder Telefon dem Datenschutzkoordinator bzw. dem Datenschutzbeauftragten zu melden. Der Datenschutzkoordinator – in seiner Abwesenheit, der Datenschutzbeauftragte – hat den kantonalen Datenschutzbeauftragten nach Vorgaben des IDG zu kontaktieren und die entsprechenden Schritte vorzunehmen.

Art. 11 Aufbewahrungsdauer

[1] Personendaten werden so lange aufbewahrt, wie sie zur Erfüllung der Aufgabe benötigt werden (laufende Ablage), d.h. in der Regel solange die Einwohnerin oder der Einwohner in der Stadt Kloten wohnt. Wenn die Personendaten nicht mehr benötigt werden, beispielsweise weil die Person nicht mehr in der Stadt Koten wohnt, gilt eine maximal folgende Aufbewahrungsfrist von 10 Jahren, mit Ausnahme spezialgesetzlicher Regelungen (ruhende Ablage).

[2] Anschliessend müssen die für das Archiv bestimmten Akten aussortiert und archiviert werden. Die nicht ins Archiv überführten Akten sind zu vernichten.

Art. 12 Umgang mit Personaldaten

[1] Für alle Mitarbeitenden wird ein elektronisches Personaldossier geführt. Es kann in Haupt- und Nebendossiers eingeteilt werden. Die Personaldossiers werden in einem zentralen Personalmanagementsystem geführt.

[2] Personalunterlagen dürfen ausserhalb des Personaldossiers ausschliesslich zum eigenen Gebrauch, als persönliche Arbeitshilfe oder als Gedächtnisstütze bearbeitet werden. Sie müssen vernichtet werden, wenn sie ihren Zweck erfüllt haben.

[3] Verantwortlichkeit:

a. Die OE Personaldienst und Finanzen betreiben ein zentrales Personalmanagement- und Lohnadministrationssystem. Die Bereichsleitung F+L erlässt Bestimmungen über das Personalmanagement- und Lohnadministrationssystem.
b. Sie regelt insbesondere:
    1. die Organisation und den Betrieb;
    2. die Zugriffsrechte;
    3. die Kategorien der gespeicherten Daten;
    4. die Massnahmen der Datensicherheit.
c. Die OE-Leitungen Personaldienst und Finanzen setzen die Sicherheitsmassnahmen zum Schutz der Personaldaten um.
d. Die Leitung Personaldienst ist für die Personaldossiers hauptverantwortlich. Er/sie entscheidet insbesondere über die Gewährung von Zugriffsrechten und setzt die angeordneten Sicherheitsmassnahmen zum Schutz der Personaldaten um. Bereichsleiter erhalten Zugriff auf diejenigen Daten, die sie im Rahmen ihrer Leitungsfunktion und des Vorgesetztenverhältnisses benötigen. Auf Daten wie Strafregisterauszüge, Scheidungsurkunden etc. erhalten sie keinen Zugriff. Diese werden in einem geschützten Bereich abgelegt. Falls Daten aus diesem Bereich das Arbeitsverhältnis betreffen, informiert der Personaldienst den Bereichsleiter.

[4] Bearbeiten von Personaldaten: Personaldaten dürfen nur so weit bearbeitet werden, als dies aus betrieblichen Gründen, namentlich im Hinblick auf die Abklärung der Eignung für das Arbeitsverhältnis, die ordnungsgemässe Durchführung des Arbeitsvertrags, zur Beendigung sowie zur Erfüllung damit verbundener gesetzlicher Pflichten notwendig ist.

[5] Aufbewahrung- und Dauer der Aufbewahrung:

a. Das Personaldossier wird durch organisatorische und technische Massnahmen vor dem Zugriff, der Einsichtnahme und vor Veränderungen durch unbefugte Personen geschützt.

b. Personaldaten sind während der Anstellung so lange aufzubewahren, wie sie für das aktuelle Arbeitsverhältnis benötigt werden, um das Arbeitsverhältnis gemäss Personalrecht abzuwickeln. Bei Beendigung des Arbeitsverhältnisses werden aus dem Personaldossier alle Unterlagen ausgesondert, die nicht mehr aufgrund gesetzlicher Aufbewahrungspflichten, für die Erteilung von Referenzauskünften oder im Zusammenhang mit Ansprüchen aus dem Arbeitsverhältnis notwendig sind. Die Aufbewahrungspflicht dauert grundsätzlich 10 Jahre nach Beendigung des Arbeitsverhältnisses. Der Personaldienst unterhält eine Checkliste der Dauer der Aufbewahrungspflicht, diese richtet sich grundsätzliche nach denjenigen Richtlinien des Kantons Zürich. Die Personaldossiers sind alle drei Jahre einer Triage zu unterziehen

[6] Einsichtsrecht: Der Personaldienst gewährt Mitarbeitenden auf Gesuch Einsicht in ihr eigenes Personaldossier. Er gewährt Vorgesetzten Einsicht in die Daten, die direkten Zusammenhang mit dem Arbeitsverhältnis haben. Das Einsichtsrecht kann eingeschränkt werden, wenn überwiegende öffentliche oder private Interessen entgegenstehen.

[7] Bewerbungsprozess: Für den Bewerbungsprozess gilt Folgendes:

a. Bewerbungsunterlagen werden im Rekrutierungsprozess nur von der für die Stellenbesetzung zuständigen Person und nur so weit bearbeitet, als dies für den betreffenden Stellenbesetzungsprozess zur Beurteilung der Eignung für das Anstellungsverhältnis notwendig und geeignet ist (Verhältnismässigkeitsprinzip). Notwendig und geeignet sind insbesondere Informationen über die fachliche und persönliche Eignung eines Bewerbers für die Ausübung der ausgeschriebenen Stelle.

b. Referenzen dürfen nur mit Zustimmung der Bewerber eingeholt und erteilt werden. Eine Zustimmung der Bewerber zu Referenzauskünften kann nicht bereits darin erblickt werden, dass sie ihre Bewerbungen Arbeitszeugnisse beigelegt haben. Als Einverständnis darf erst die ausdrückliche Nennung der früheren Arbeitgeber oder Vorgesetzten als Referenzpersonen durch die Bewerbenden angesehen werden. Für Stellenbewerbende muss erkennbar sein, dass Daten bei Referenzpersonen eingeholt werden (Transparenzprinzip).

c. Bewerbenden dürfen nur Fragen gestellt werden, die sich auf die Eignung für die zukünftigen beruflichen Aufgaben beziehen oder sonstige Sachverhalte betreffen, die für die Erfüllung des Arbeitsvertrags von Bedeutung sind (z.B. besondere Stärken/Schwächen). Fragen, welche die Privatsphäre betreffen und nicht in direktem Zusammenhang mit dem Arbeitsverhältnis stehen (z.B. Familiengründung, finanzielle Verhältnisse, Gesundheit, Religion, politische oder sexuelle Orientierung), sind nicht zulässig.

d. Die Unterlagen von Bewerbenden, die nicht angestellt werden sowie jegliche Kopien davon sind nach Beendigung des Rekrutierungsprozesses innerhalb von drei bis sechs Monaten unwiderruflich zu vernichten bzw. zu löschen und die Mitarbeitenden, die eine Kopie der Bewerbungsunterlagen erhalten haben, über diese Pflicht zur Löschung zu informieren.

e. Sämtliche Mitarbeitenden ausserhalb des Personaldienstes, die eine Arbeitskopie der Bewerbungsunterlagen oder Zugriff darauf erhalten haben, müssen diese nach Abschluss des Rekrutierungsprozesses unwiderruflich vernichten bzw. löschen, unabhängig davon, ob die Bewerbenden angestellt wurden oder nicht. Falls Bewerbungsunterlagen für eine Anstellung in einer anderen Position in Frage kommen, muss vor der Weiterleitung der Unterlagen die Einwilligung der Bewerbenden eingeholt werden.

[8] Im Weiteren gilt das Merkblatt «Online-Recherchen über Stellenbewerbende» des Datenschutzbeauftragten des Kantons Zürich.

Art. 13 Daten der Einwohnerkontrolle

[1] Für den Umgang mit Personendaten der Einwohnerkontrolle gelten die folgenden zusätzlichen Vorgaben:

a. Abrufverfahren aus dem Einwohnerregister: Die Stadt Kloten kann einem anderen öffentlichen Organ mittels elektronischem Abrufverfahren einen Online-Zugriff auf das Einwohnerregister gewähren. § 17 MERG stellt eine gesetzliche Grundlage für ein gemeindeeigenes elektronisches Abrufverfahren dar. Für die Gewährung von Online-Zugriffen gilt der Verhältnismässigkeitsgrundsatz. Es dürfen nicht alle eingetragenen Merkmale freigeschaltet werden, sondern nur jene, welche für die konkrete Aufgabenerfüllung des Datenempfängers erforderlich sind.

b. Bekanntgabe an Private:
   1. Die Einwohnerkontrolle ist in gewissen Fällen verpflichtet oder berechtigt, Daten an Privatpersonen oder Organisationen herauszugeben. Neben der Prüfung der in den §§ 18 f. MERG genannten Voraussetzungen ist aber immer auch eine Interessenabwägung nach § 23 IDG vorzunehmen.
   2. Folgende Daten dürfen auf Ersuchen und im Einzelfall voraussetzungslos, d.h. ohne dass der Gesuchsteller das Gesuch begründen muss, bekannt gegeben werden: Name, Vorname, Adresse, Datum von Zu- und Wegzug.

3. Wird ein berechtigtes Interesse[1)] glaubhaft gemacht, werden zusätzlich folgende Personendaten (sogenannte «erweiterte Personalien») bekannt gegeben: Zuzugsort und Wegzugsort, Geburtsdatum, Geschlecht, Zivilstand, Heimatort.

[2] Im Weiteren gilt der Leitfaden «Datenschutzlexikon Einwohnerkontrollen» des Datenschutzbeauftragten des Kantons Zürich.

Art. 14 Daten des Pflegezentrums

[1] Im Umgang mit Pflege- und Patientendaten gilt das Gesundheitsgesetz (GesG) des Kantons Zürich. Es enthält Regelungen zur Schweigepflicht und zum Führen von Patientendokumentationen.

Art. 15 Sensibilisierung und Schulung der Mitarbeitenden

[1] Alle Mitarbeitenden werden im Rahmen der Mitarbeitereinführung auf das Datenschutzreglement hingewiesen und regelmässig geschult. Jede Abteilung unterstützt ihre Mitarbeitenden bei den betreffenden Prozessen.

Art. 16 Organisation

[1] Stadtrat: Der Stadtrat der Stadt Kloten definiert im Rahmen des vorliegenden Datenschutzreglements die Grundsätze für die Gewährleistung des Datenschutzes bei der Stadt Kloten. Er ernennt eine datenschutzverantwortliche Person, den Datenschutzkoordinator, der mit der Durchsetzung der datenschutzrechtlichen Vorgaben beauftragt wird.

[2] Datenschutzkoordinator:

a. Der Datenschutzkoordinator ist die interne Ansprechstelle für den Datenschutz in der Stadt Kloten und wird durch den externen Datenschutzbeauftragten unterstützt.
b. Der Datenschutzkoordinator und der externe Datenschutzbeauftragte informieren den Stadtrat jährlich über ihre Tätigkeit und den Stand des Datenschutzes bei der Stadt Kloten.

[1)] Ein berechtigtes Interesse wird angenommen, wenn die anfragende Person beabsichtigt, mit dem Einwohner aus einleuchtenden Gründen in Beziehung zu treten. Eine Bekanntgabe von erweiterten Personalien ist ausgeschlossen, wenn dies rechtsmissbräuchlich (d.h. in Umgehung oder Verletzung einer Vorschrift) geschieht, sowie bei reiner Neugier. Diese Beziehung kann von geschäftlicher (Vertrag, Überprüfung der Angaben einer Person, die eine Kreditkarte beantragt hat), persönlicher (Freundschaft), kultureller (Vereine, Veranstaltungen) oder anderer Art sein.

c. Der Datenschutzkoordinator und der externe Datenschutzbeauftragte arbeiten eng mit den für Informationssicherheit zuständigen Stellen der Stadt Kloten zusammen.

d. Der Datenschutzkoordinator und der externe Datenschutzbeauftragte bilden zusammen die Datenschutzorganisation der Stadt Kloten.

[3] Datenschutzbeauftragter:

a. Der Datenschutzbeauftragte ist die externe Ansprechstelle für den Datenschutz. Er unterstützt den Datenschutzkoordinator bei der Durchsetzung und Umsetzung des Datenschutzes. Dabei berät er den Datenschutzkoordinator in fachlicher Hinsicht.

b. Er unterstützt die Umsetzung und Überwachung der datenschutzrechtlichen Vorgaben innerhalb der Stadt Kloten.

[4] Leitung Personaldienst: Die Leitung Personaldienst und die im Personaldienst tätigen Mitarbeitenden sind für die sorgfältige und datenschutzkonforme Bearbeitung der Personaldaten verantwortlich.

[5] Leiter Informatik: Der/die Leiter/in Informatik trägt die Verantwortung, dass die Datensicherheit und datenschutzrechtliche Massnahmen technisch umgesetzt werden. Dabei unterstützen ihn/sie insbesondere die Applikations- und Systemverantwortlichen. Der/die Leiter/in Informatik arbeitet eng mit der Datenschutzorganisation zusammen, um die Konformität der Massnahmen zu prüfen. So beurteilen sie Risiken, Vorfälle und Beinahe-Vorfälle, welche den Datenschutz gefährden können.

[6] Vorgesetzte: Die Vorgesetzten aller Stufen sind in ihren Verantwortungsbereichen für die Durchsetzung und Einhaltung des Datenschutzes verantwortlich, insbesondere im Rahmen der Geschäftsprozesse. Sie sorgen in Zusammenarbeit mit der Datenschutzorganisation für Schulung und Sensibilisierung der Mitarbeitenden. Sie nehmen eine Vorbildfunktion wahr und fördern die Motivation der Mitarbeitenden, Massnahmen zum Datenschutz einzuhalten.

[7] Dateneigner: Dateneigner der jeweiligen Abteilungen sind verantwortlich für die Klassifizierung der Informationen und Daten und die Anwendung von angemessenen Schutzmassnahmen. Sie bestimmen über Zugriff, Veränderung oder Weitergabe der Daten und schützen diese mit entsprechenden Massnahmen vor unerlaubten Zugriffen. Bei elektronischen Daten haben sie im Austausch mit der IT die Einhaltung der datenschutzrechtlichen Anforderungen in technischer und organisatorischer Hinsicht sicherzustellen.

[8] Projektleitende: Projektleitende sind im Rahmen ihrer Projekte verantwortlich für die Klassifizierung der Daten und die Anwendung von angemessenen Schutzmassnahmen.

[9] Mitarbeitende:

a. Sämtliche Mitarbeitenden sind für den Datenschutz verantwortlich und verpflichtet, Personendaten nach den intern und gesetzlich vorgegebenen Bestimmungen zu bearbeiten. Kritische Aufmerksamkeit und eigenverantwortliches Verhalten werden vorausgesetzt. Mitarbeitende können sich bei Unklarheiten oder für Auskünfte jederzeit an ihre Vorgesetzten, den Datenschutzkoordinator oder bei dessen Abwesenheit an den Datenschutzbeauftragten wenden.

b. Mitarbeitende erhalten hinsichtlich ihrer Verantwortung für den Datenschutz und ihrer Tätigkeit die entsprechende Sensibilisierung und Ausbildung. Sie erhalten Zugriff auf Dokumente, Formulare, Meldungen und Informationen zum Thema Datenschutz über die entsprechende Intranet-Seite oder andere zugängliche Medien.

Art. 17 Sanktionen

[1] Verletzungen dieses Datenschutzreglements können disziplinarische Sanktionierungen, zivil-, verwaltungs- oder strafrechtliche Massnahmen nach sich ziehen.

Art. 18 Schlussbestimmungen

[1] Das Datenschutzreglement ist allen Mitarbeitenden über das Intranet zugänglich. Über relevante Änderungen oder Ergänzungen zu diesem Reglement werden die Mitarbeitenden in geeigneter Form informiert. Änderungen oder Ergänzungen treten im Moment der Publizierung auf dem Intranet in Kraft.

II.

Keine Fremdänderungen.

III.

Der Erlass SRS 1.2-2 (Datenschutzreglement vom 12. Dezember 1995) wird aufgehoben.

IV.

Dieses Reglement tritt am 1. Juni in Kraft.

Kloten, 24.05. 2022

Präsident: René Huber
Verwaltungsdirektor: Thomas Peter