Inhalt

1 Ziel und Zweck ... 2
2 Geltungsbereich ... 2
3 Gesetzliche Grundlagen ... 2
4 Begriffserklärungen ... 2
5 Grundsätze der Datenbearbeitung ... 4
6 Datenschutzorganisation ... 5
7 Datenschutz durch Technik (Privacy by Design) und datenschutzfreundliche Voreinstellungen (Privacy by Default) ... 6
8 Bearbeitungsverzeichnis ... 6
9 Datenschutz-Folgenabschätzung ... 6
10 Informationspflichten ... 7
11 Datenbekanntgabe und Datenbearbeitung durch Auftragsbearbeiter ... 7
12 Datensicherheit ... 7
12.1 Technischer und organisatorischer Schutz ... 7
12.2 Verletzungen der Datensicherheit ... 8
13 Rechte betroffener Personen ... 8
13.1 Auskunftsrecht ... 8
13.2 Löschbegehren ... 8
13.3 Berichtigung, Sperrung und Portabilität ... 8
13.4 Koordination der Begehren ... 9
14 Datenschutzrevers (Anhang zu dieser Weisung) ... 9
15 Weitere Weisungen zum Thema Umgang mit Informationen ... 9
Anhang Datenschutz-Revers ... 10

1 Ziel und Zweck

Mit der Gruppenweisung Datenschutz sollen folgende Ziele erreicht werden:

- Schaffung eines einheitlichen Mindeststandards im Umgang mit Personendaten innerhalb der EKZ-Gruppe;
- Schutz der Persönlichkeitsrechte und der Privatsphäre von Mitarbeitenden, Kunden, Geschäftspartnern, Lieferanten und Stellenbewerbenden;
- Erreichen eines angemessenen Datenschutzniveaus gemäss den gesetzlichen Anforderungen;
- verbindliche Festlegung der Verantwortlichkeiten.

2 Geltungsbereich

Sämtliche Mitarbeitende der EKZ-Gruppe haben diese Weisung einzuhalten.

3 Gesetzliche Grundlagen

Als öffentlich-rechtliche Anstalt des Kantons Zürich gelangen für die EKZ das Gesetz über die Information und den Datenschutz (IDG) sowie die zugehörige Verordnung über die Information und den Datenschutz (IDV) für diejenigen Tätigkeiten zur Anwendung, welche *nicht* am wirtschaftlichen Wettbewerb teilnehmen und dabei *nicht* hoheitlich handeln.

Handeln die EKZ in einem abgegrenzten Geschäftsfeld im freien Wettbewerb rein privatrechtlich (Prosumer, EKZ Eltop AG, Contracting, usw.), gelangt das Bundesgesetz über den Datenschutz (DSG) zur Anwendung.

Die Datenschutzgrundverordnung der Europäischen Union (DSGVO) kann punktuell auch für die EKZ-Gruppe gelten. Erbringen EKZ Dienstleistungen oder liefern EKZ Waren für Endkunden in der EU oder werden im Internet Tracking-Tools eingesetzt, welche Bewohner des EU/EWR-Raumes tracken, ist die Fachstelle Datenschutz davon in Kenntnis zu setzen, um die Anwendbarkeit der DSGVO zu prüfen.

4 Begriffserklärungen

Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.
Betroffene Personen	Personen, deren Daten bearbeitet werden.
Gewöhnliche Personendaten	Personendaten, deren Informationsgehalt in der Regel kein besonderes Risiko einer Stigmatisierung oder Diskriminierung für die betroffene Person mit sich bringt.

Besonders schützenswerte Personendaten	Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht. Dies betrifft insbesondere «sensitive» Personendaten wie: ▪ Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten ▪ Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie ▪ genetische Daten ▪ biometrische Daten, die eine natürliche Person eindeutig identifizieren ▪ Daten über Massnahmen der sozialen Hilfe wie z.B. Fürsorgegeldempfänger ▪ Daten über verwaltungs- und strafrechtliche Verfolgungen und Sanktionen ▪ Zusammenstellungen von Informationen, welche eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben.
Bearbeiten	Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln oder Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.
Bekanntgeben	Das Zugänglichmachen von Personendaten wie das Einsichtsgewähren, Weitergeben oder Veröffentlichen.
Datenschutzberater/in	Unabhängige Stelle, welche die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht.
Profiling	Die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen.
Verletzung der Datensicherheit	Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.
Verantwortlicher	Person, die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.
Auftragsbearbeiter (der EKZ)	Natürliche oder juristische Person, die im Auftrag der EKZ tätig wird und hierfür Personendaten aus dem Besitz der EKZ bearbeitet bzw. zur Auftragserfüllung zwingend auf die Angaben von Personendaten der EKZ angewiesen ist.

Datenschutzfolgenabschätzung	Eine strukturierte Risikoanalyse bezüglich eines geplanten Datenverarbeitungsprozesses.

5 Grundsätze der Datenbearbeitung

Die Bearbeitung von Personendaten muss jederzeit sorgfältig und gewissenhaft gemäss den nachfolgenden Grundsätzen erfolgen. Insbesondere ist bei der Bearbeitung auf sachliche Richtigkeit und respektvollen Ton zu achten.

- **Fairness**: Datenbearbeitungen erfolgen nur im Rahmen der berechtigten Erwartungen der betroffenen Person (Treu und Glauben). *Beispiel: Das heimliche Aufnehmen von Telefonaten ist strikte untersagt. Personendaten sind transparent bei der betroffenen Person zu beschaffen.*

- **Rechtmässigkeit**: Jede Datenbearbeitung muss sich auf eine genügende Rechtsgrundlage stützen. In den Bereichen, in welchen die EKZ hoheitlich tätig wird, bedarf die Bearbeitung von besonderen Personendaten / besonders schützenswerten Personendaten einer hinreichend bestimmten Regelung in einem formellen Gesetz.

- **Transparenz**: Details der Datenbearbeitung müssen den betroffenen Personen verständlich erklärt werden. Die EKZ informiert die betroffenen Personen in der Regel über Datenschutzerklärungen oder in einer anderen geeigneten Form. Dabei muss über jede Beschaffung von Personendaten informiert werden.

- **Zweckbindung**: Die Datenbearbeitung erfolgt nur zu dem transparent angegebenen Zweck oder damit vereinbaren Zwecken. Die Bearbeitung muss dabei immer verhältnismässig sein. *Beispiel: Werden Adressdaten, welche aufgrund einer Wettbewerbsteilnahme der EKZ mitgeteilt wurden, später z.B. zu Marketingzwecken verwendet, muss der Teilnehmer hierzu ausdrücklich seine Zustimmung erteilt haben. Andernfalls werden die auf dem Wettbewerbstalon mitgeteilten Daten zweckentfremdet.*

- **Datenminimierung**: Es werden nur so viele Daten erhoben und bearbeitet, wie für die Zweckerfüllung erforderlich sind. Zu diesem Grundsatz gehört auch, dass nur diejenigen Personen Zugriff auf die Daten haben, deren Zugriff für die Zweckerfüllung tatsächlich notwendig ist.

- **Speicherbegrenzung**: Daten werden nur so lange gespeichert wie nötig. Vor der Löschung sind die Interessen der EKZ (z.B. Geltendmachung von Rechtsansprüchen, gesetzliche Aufbewahrungsfristen etc.) mit den Interessen der betroffenen Person abzugleichen.

- **Richtigkeit**: Fehlerhafte Daten sind zeitnah zu löschen oder zu korrigieren.

- **Sicherheit**: Es ist ein angemessener Schutz gegen Vernichtung, Verlust, Veränderung oder unbefugte Offenbarung der Daten zu gewährleisten.

Wichtig!
Besondere Sorgfalt im Umgang mit den Personendaten ist geboten, wenn uns diese von den Betroffenen selber oder von Gemeinden, Verwaltungen, etc. bekannt gegeben werden, obwohl sie für das Vertragsverhältnis nicht notwendig sind. Darunter fallen unter anderem Angaben in Scheidungsurteilen, Betreibungsurkunden, Sterbeurkunden etc. Derartige Angaben dürfen in keinem Fall Dritten weitergegeben werden. Allfällige Originaldokumente sind an den Eigentümer zu retournieren.

6 Datenschutzorganisation

Geschäftsleitung	Die Geschäftsleitung ist verantwortlich für die Durch- und Umsetzung des Datenschutzes und erlässt die vorliegende Datenschutzweisung sowie sich daraus ableitende Dokumente.
Fachstelle Datenschutz	Die Fachstelle Datenschutz wird vertreten durch den/die Datenschutzberater/in und unterstützt die EKZ fachlich unabhängig und weisungsungebunden bei der Durch- und Umsetzung des Datenschutzes. Die Fachstelle Datenschutz nimmt die folgenden Aufgaben wahr: ▪ Prüft die Bearbeitung von Personendaten und empfiehlt Korrekturmassnahmen, wenn Datenschutzvorschriften verletzt werden. ▪ Mitwirkung bei der Erstellung von Datenschutz-Folgeabschätzungen und deren Überprüfung ▪ Meldung von Verletzungen der Datensicherheit ▪ Anlaufstelle für betroffene Personen ▪ Schulung und Beratung von Mitarbeitenden in Fragen des Datenschutzes
Personalabteilung	Die Personalabteilung ist zuständig für die sorgfältige und datenschutzkonforme Bearbeitung der Personendaten von aktuellen und ehemaligen Mitarbeitenden sowie Stellenbewerbenden.
Informatik	Die Informatik ist zuständig für die Umsetzung der technischen Massnahmen im Bereich der IT-Systeme. Dabei unterstützt sie insbesondere die Informatik- und Businessverantwortlichen. Sie arbeitet eng mit der Fachstelle Datenschutz zusammen.
Vorgesetzte	Die Vorgesetzten sind in ihrem Verantwortungsbereich zuständig für die Einhaltung und Durchsetzung des Datenschutzes.
Mitarbeitende	Die Mitarbeitenden sind in ihren Verantwortungsbereichen zuständig für die Umsetzung und Einhaltung des Datenschutzes. Bei Verdacht eines Datenschutzvorfalls (z. B. dass Personendaten unter Verletzung gesetzlicher Datenschutzbestimmungen verwendet wurden oder die Sicherheit von Systemen, welche Personendaten enthalten, nicht mehr gewährleistet ist) benachrichtigen sie die Fachstelle Datenschutz.

7 Datenschutz durch Technik (Privacy by Design) und datenschutzfreundliche Voreinstellungen (Privacy by Default)

Die EKZ gestaltet die Datenbearbeitung technisch und organisatorisch so aus, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze der Datenbearbeitung nach Ziff. 5 der vorliegenden Datenschutzweisung. Für technische Systeme ist der Datenschutz ab der Planung einzubeziehen.

Die EKZ stellt mittels geeigneter Voreinstellungen sicher, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt. Der Bearbeitungsvorgang ist standardmässig möglichst datenschutzfreundlich einzurichten.

8 Bearbeitungsverzeichnis

Die EKZ führt das gesetzlich vorgeschriebene Bearbeitungsverzeichnis. Die Mitarbeitenden unterstützen die EKZ hierzu in ihrem Zuständigkeitsbereich angemessen. D.h. jeder bzw. jede Businessverantwortliche pflegt neue Bearbeitungstätigkeiten (z. B. Einführung neue Software, welche u. a. Kundendaten bearbeitet oder Software zur Erstellung von Offerten) vor deren Eröffnung bzw. Aufnahme der Bearbeitungstätigkeit im Bearbeitungsverzeichnis ein.

Wesentliche Änderungen an der Datenbearbeitung (insbesondere das Löschen von Datensammlungen oder wenn neue Bearbeitungen mit besonders schützenswerten Personendaten aufgenommen werden) meldet der oder die Businessverantwortliche möglichst frühzeitig der Fachstelle Datenschutz und der IT.

9 Datenschutz-Folgenabschätzung

Sofern eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann, erstellt die EKZ vorgängig eine Datenschutz-Folgenabschätzung. Die Datenschutz-Folgeabschätzung hat im Minimum eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte zu enthalten.

Die Mitarbeitenden unterstützen die EKZ bei der Erstellung der Datenschutz-Folgenabschätzung, indem sie die Fachstelle Datenschutz so früh wie möglich über die geplante Bearbeitung informieren, so dass geprüft werden kann, ob eine Datenschutz-Folgenabschätzung erforderlich ist.

Sind besondere Risikofaktoren anhand der Datenschutz-Folgenabschätzung identifiziert worden und ist die Datenbearbeitung im Anwendungsbereich des IDG geplant (vgl. Ziff. 3), ist das Vorhaben der Datenschutzbeauftragten des Kantons Zürich zur Vorabkontrolle einzureichen.

10 Informationspflichten

Die EKZ teilt den betroffenen Personen bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit die betroffenen Personen ihre Rechte geltend machen können und eine transparente Datenbearbeitung gewährleistet ist.

Die Mitarbeitenden unterstützen die EKZ hinsichtlich ihren Informationspflichten, indem sie insbesondere

- den Bearbeitungszweck und die Kategorien der Bearbeitung,
- gegebenenfalls die Empfänger der Personendaten und
- gegebenenfalls den Staat oder die Organisation, an den oder an die die Personendaten bekanntgegeben werden,

mitteilen. Die Information an die betroffenen Personen erfolgt in der Regel über die Datenschutzerklärungen.

11 Datenbekanntgabe und Datenbearbeitung durch Auftragsbearbeiter

Ob eine Bekanntgabe von Personendaten ins Ausland oder eine Bearbeitung durch Dritte erlaubt ist, ist mit der Fachstelle Datenschutz abzustimmen. Bei Zulässigkeit sind dem Dritten die notwendigen Datenschutzpflichten vertraglich zu überbinden und deren Einhaltung durch EKZ zu überwachen. Die Verantwortung über die rechtmässige Bearbeitung der weitergegebenen Daten verbleibt in jedem Fall bei EKZ.

12 Datensicherheit

12.1 Technischer und organisatorischer Schutz

Durch technische und organisatorische Massnahmen sind die Vertraulichkeit, Verfügbarkeit und Integrität der Personendaten zu gewährleisten. Insbesondere ist der Schutz der Systeme und der physischen Datenträger vor unbefugter oder zufälliger Vernichtung, zufälligem Verlust, technischem Fehler, Fälschung, Diebstahl oder widerrechtlicher Verwendung, unbefugtem Ändern, Kopieren oder Zugreifen durch jeden Mitarbeitenden sicherzustellen.

Die Massnahmen orientieren sich am Stand der Technik, den von der Bearbeitung ausgehenden Risiken und dem Schutzbedarf der Personendaten. Sie werden kontinuierlich überprüft, bewertet und wo notwendig angepasst.

12.2 Verletzungen der Datensicherheit

Die Mitarbeitenden melden sicherheitsrelevante Vorfälle unverzüglich. Der Einbezug der Fachstelle Datenschutz wird fallbezogen geprüft.

- Geräte, die von Avenique verwaltet werden:
  IT-Hotline: T+41 (0) 800 55 05 05 / hotline@aveniq.ch

- Geräte, die von EKZ verwaltet werden:
  EKZ Incident Response Team: T +41 (0)58 359 56 07 / EKZ-IR@ekz.ch

13 Rechte betroffener Personen

13.1 Auskunftsrecht

Betroffene Personen können Auskunft darüber verlangen, ob und welche Personendaten über sie bearbeitet werden. Die betroffene Person erhält auf schriftliches Verlangen hin von EKZ diejenigen Informationen, die erforderlich sind, damit die betroffene Person ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Das Auskunftsrecht umfasst:

- Die Identität und Kontaktdaten der EKZ
- Die bearbeiteten Personendaten
- Den Bearbeitungszweck
- Die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer
- Die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person erhoben wurden
- Gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht
- Gegebenenfalls die Empfängerinnen und Empfänger, denen die Personendaten bekanntgegeben werden

13.2 Löschbegehren

Vor einer Löschung werden die Interessen der EKZ mit den Interessen der betroffenen Person abgewogen sowie gesetzliche Aufbewahrungspflichten überprüft.

13.3 Berichtigung, Sperrung und Portabilität

Den betroffenen Personen steht unter Beachtung des Verhältnismässigkeitsgrundsatzes zudem das Recht auf Berichtigung und Sperrung von personenbezogenen Daten zu. Bei der Übertragung von Daten ist zudem ein portables Format zur Verfügung zu stellen.

13.4 Koordination der Begehren

Die Fachstelle Datenschutz prüft und koordiniert die Beantwortung der Begehren. Die Mitarbeitenden unterstützen sie hierbei in angemessenem Umfang.

14 Datenschutzrevers (Anhang zu dieser Weisung)

Von Mitarbeitenden mit besonderen Aufgaben kann zudem durch Unterzeichnung des Datenschutzrevers eine explizite persönliche Verpflichtungserklärung zur Einhaltung des Datenschutzes verlangt werden. Dieses unterzeichnete Revers wird in der Personalakte des entsprechenden Mitarbeitenden abgelegt.

Zwingend ist die Verpflichtungserklärung für Mitarbeitende des Personaldienstes, der Informatik, des Controllings sowie der internen Postdienste. Bei den übrigen Mitarbeitenden entscheidet der Linienvorgesetzte aufgrund der konkreten Aufgaben.

15 Weitere Weisungen zum Thema Umgang mit Informationen

- Sicherheitspolitik EKZ
- Weisung "Klassifikation"
- Weisung "Verhalten am Arbeitsplatz"
- Weisung "Archivierung"
- Weisung "Sicherer Umgang mit IT-Mitteln"
- Weisung "Internet Services"
- Weisung "Zugriffskontrolle für IT-Systeme"
- Weisung "Mobile Nutzung von IT-Mitteln"