



dsb

datenschutzbeauftragte
des kantons zürich

Zustellplattformen und Signaturdienste

Am 1. Januar 2026 treten die revidierten Bestimmungen zu den elektronischen Verfahrenshandlungen im Verwaltungsverfahren in Kraft, welche die öffentlichen Organe verpflichten, elektronische Eingabe- und Zustellwege anzubieten. Elektronisch zugestellte Anordnungen (Verfügungen) müssen ausserdem vom öffentlichen Organ elektronisch signiert werden. Bei der Wahl der benötigten Software sind Datenschutzaspekte im Rahmen einer Datenschutz-Folgenabschätzung (DSFA) frühzeitig zu beachten. Gegebenenfalls ist auch eine Vorabkontrolle bei der Datenschutzbeauftragten durchzuführen.

1 Elektronische Verfahrenshandlungen

Das revidierte Verwaltungsrechtspflegegesetz des Kantons Zürich (VRG, [LS 175.2](#)) sieht vor, dass Verwaltungsbehörden elektronisch erreichbar sind. Die Verwaltungsbehörde bestimmt den für sie massgeblichen Kanal (§ 4e Abs. 1 VRG). Die Verordnung über elektronische Verfahrenshandlungen im Verwaltungsverfahren (VEVV, [LS 175.26](#)) regelt, welche Voraussetzungen dieser Kanal erfüllen muss. Darin ist festgehalten, dass die Übermittlungen vor unrechtmässiger Kenntnisnahme zu schützen sind. Auch ist eine unveränderte Übermittlung der Informationen zu gewährleisten. Der Zeitpunkt der Abgabe von Eingaben ist eindeutig festzustellen und zu quittieren. Dies trifft auch auf den erstmaligen Abruf von Anordnungen zu.

Folgende vom Bund anerkannten Zustellplattformen erfüllen diese Kriterien:

- PrivaSphere Secure Messaging der PrivaSphere AG,
- IncaMail der Schweizerischen Post AG.

Alternativ zu den vom Bund anerkannten Zustellplattformen können Verwaltungsbehörden andere Kanäle für bestimmte Rechtsgebiete oder Verfahrensarten einrichten und kommunizieren. Diese müssen die Kriterien ebenfalls erfüllen.

Das revidierte VRG sieht weiter vor, dass öffentliche Organe Anordnungen (Verfügungen) elektronisch ausstellen müssen, wenn die Partei dies wünscht, beziehungsweise die Eingabe elektronisch erfolgt ist. Die elektronische Verfügung ist vom öffentlichen Organ mit einer qualifizierten Elektronischen Signatur (QES) oder einem geregelten elektronischen Siegel gemäss Bundesgesetz über die elektronische Signatur ([ZertES, SR 943.03](#)) zu versehen.

2 Vorgehen

Ein öffentliches Organ des Kantons Zürich bewertet bei einer beabsichtigten Bearbeitung von Personendaten deren Risiken für die Grundrechte der betroffenen Personen (Datenschutz-Folgenabschätzung, § 10 Abs. 1 Gesetz über die Information und den Datenschutz, IDG, [LS 170.4](#)). Diese vorgängige Einschätzung der Risiken der geplanten Datenbearbeitung kann mit einem [DSFA-Formular](#) durchgeführt werden.

Ergibt die Einschätzung, dass besondere Risiken für die Grundrechte der betroffenen Personen vorliegen, unterbreitet das öffentliche Organ das Vorhaben vorab der Datenschutzbeauftragten zur Prüfung (Vorabkontrolle, § 10 Abs. 2 IDG). Einige dieser Risikofaktoren sind in § 24 der Verordnung über die Information und den Datenschutz (IDV, [LS 170.41](#)) aufgezählt.

Auch bei der Wahl der Zustellplattform sowie der Signaturdienste schätzt das öffentliche Organ diese Risiken ein und unterbreitet das Projekt bei Vorliegen besonderer Risiken der Datenschutzbeauftragten zur Vorabkontrolle.

Zustellplattformen

Bei den vom Bund anerkannten Zustellplattformen wurden im Rahmen der Anerkennung Datenschutzaspekte bereits geprüft (vgl. [Informationen des Bundes zur Elektronischen Übermittlung](#)). Möchten öffentliche Organe des Kantons Zürich für elektronischen Verfahrenshandlungen eine der anerkannten Zustellplattformen des Bundes einsetzen, ist weder eine DSFA durchzuführen, noch das Vorhaben der Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

Entscheidet sich ein öffentliches Organ für die Wahl eines anderen Kanals, muss dieser die Anforderungen nach § 2 Abs. 2 VEVV erfüllen. Ausserdem ist mittels DSFA zu prüfen, ob besondere Risiken für die Grundrechte der Betroffenen bestehen. Gegebenenfalls ist eine Vorabkontrolle durchzuführen. In diesem Fall ist auch die Erstellung eines ISDS-Konzepts sowie einer Rechtsgrundlagenanalyse notwendig.

Signaturdienste

Verschiedene Signaturlösungen ermöglichen das elektronische Signieren mit Signaturzertifikaten nach dem Bundesgesetz über die elektronische Signatur (ZertES). Sie weisen dabei unterschiedliche Funktionalitäten auf (z.B. Integration eines Signatur-Workflows, um weitere Signierende einzuladen).

Unabhängig vom gewählten Signaturzertifikat ist mittels DSFA zu prüfen, ob die eingesetzte Software datenschutzkonform ist und ob eine Vorabkontrolle durchzuführen ist. Sollen beispielsweise Signaturdienste genutzt werden, die das Hochladen von Dokumenten in eine Cloud zwecks Unterzeichnung ermöglichen, ist die geplante Bearbeitung der Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten.

3 Weitere Informationen

Nähere Informationen zur Umsetzung der revidierten Bestimmungen des VRG sowie der VEVV können der [Website des Kantons Zürich](#) entnommen werden.

V 1.0 / April 2025