

DATENSCHUTZERKLÄRUNG

**EU-Datenschutz-Grundverordnung (2016/679),
Artikel 12-14**

Datum: 29.4.2025, v3

Aidian Oy verpflichtet sich, die Privatsphäre zu schützen und personenbezogene Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen und guten Datenschutzpraktiken zu verarbeiten. Diese Datenschutzerklärung beschreibt, wie Aidian die personenbezogenen Daten der Person, die einen Verdacht auf Fehlverhalten gemeldet hat (die sogenannte Whistleblowing-Meldung) (der "Meldende") und die personenbezogenen Daten der Person, die Gegenstand der Whistleblowing-Meldung ist (der "Gemeldete"), erhebt, verarbeitet und schützt. Die Meldung kann anonym eingereicht werden, aber es ist möglich, dass die Identität des Meldenden einer anonymen Meldung auch indirekt aus den Informationen hervorgeht, die der Meldende in der Meldung gemacht hat. Aidian versucht jedoch nicht, den Reporter zu identifizieren, es sei denn, es ist für die Untersuchung der Angelegenheit absolut notwendig.

Wir behalten uns das Recht vor, diese Datenschutzerklärung jederzeit zu aktualisieren oder zu ändern, und wenn dies gesetzlich vorgeschrieben ist, werden wir die betroffenen Personen darüber informieren.

1. Verantwortlicher und/oder gemeinsam Verantwortlicher	Aidian Oy Koivu-Mankkaan Krawatte 6B 02200 Espoo Finnland Tel. +358 10 309 300 Unternehmens-ID: 1855216-1
2. Kontaktdaten für datenschutzrechtliche Angelegenheiten	Datenschutzbeauftragter: E-Mail-Adresse: dataprotection@aidian.eu Telefon: 010 309 3000 (Mitte) Postanschrift: Aidian Oy / Data protection issues, Koivu-Mankkaan tie 6B, 02200 Espoo
3. Name des Registers	Der Whistleblowing-Kanal von Aidian und der Prozess zur Lösung der Whistleblowing-Meldungen
4. Zweck der Verarbeitung personenbezogener Daten und Rechtsgrundlage für die Verarbeitung personenbezogener Daten	<u>Zweck der Verarbeitung personenbezogener Daten:</u> Personenbezogene Daten werden im Zusammenhang mit der Bearbeitung von Whistleblowing-Meldungen verarbeitet. Die Meldung kann anonym erfolgen. Es ist jedoch möglich, dass die Identität des Meldenden indirekt aus den in der Meldung enthaltenen Informationen hervorgeht. Darüber hinaus kann der Meldende personenbezogene Daten über die Person bereitstellen, die Gegenstand der Meldung ist. Der Zweck des Hinweisgeberkanals besteht darin, die Meldung von beobachteten oder vermuteten Aktivitäten zu ermöglichen, die gegen das öffentliche Interesse oder ethische Grundsätze im Zusammenhang mit der Arbeit verstoßen. <u>Rechtsgrundlage für die Verarbeitung personenbezogener Daten:</u> Personenbezogene Daten werden verarbeitet, um der rechtlichen Verpflichtung des Verantwortlichen nachzukommen (Art. 6 Abs. 1 lit. c DSGVO) und aus einem wichtigen Grund des öffentlichen Interesses: der Verarbeitung von Meldungen über mutmaßliches Fehlverhalten (Art. 9 Abs. 2 lit. g DSGVO). Die

	Verpflichtung basiert auf der Richtlinie 2019/1937 der Europäischen Union und der daraus resultierenden nationalen Gesetzgebung, dem Hinweisgeberschutzgesetz 1171/2022.
5. Im Register enthaltene Daten	Es ist möglich, anonym oder unter eigenem Namen zu melden. Die Meldung wird stets vertraulich behandelt, und die Identität des Meldenden ist nur den Personen bekannt, die mit der Bearbeitung der Meldungen beauftragt wurden, und den Personen, die als Sachverständige zur Untersuchung der Meldung eingeladen wurden. Das Register kann die folgenden Arten von personenbezogenen Daten über den Meldenden und den Gemeldeten sowie über andere mit der Angelegenheit verbundene Personen, wie z. B. Zeugen, enthalten: • Name, E-Mail-Adresse und Telefonnummer des Meldenden. Die Meldung kann auch völlig anonym erfolgen. • Informationen in der Meldung, einschließlich des Namens der gemeldeten Person, Informationen über mögliche illegale Aktivitäten (inkl. Ort und Zeit), Informationen über Zeugen. Informationen im Zusammenhang mit der Erstellung und Verarbeitung der Meldung sowie Nachrichten (einschließlich Benachrichtigungscode und Status). • Alle anderen Informationen, die vom Meldenden zur Verfügung gestellt werden. Die Informationen können besondere Kategorien personenbezogener Daten (z. B. Informationen über den Gesundheitszustand der Person) oder Informationen über Straftaten oder Verstöße enthalten, soweit diese im Rahmen des Ermittlungsverfahrens auftauchen. Die Anweisungen des Whistleblowing-Kanals raten dem Meldenden, die gemeldeten personenbezogenen Daten auf das Notwendige und Angemessene zu beschränken, aber da die Meldenden die Daten selbst eingeben können, hat der für die Verarbeitung Verantwortliche nicht die Möglichkeit, die in die Meldung eingegebenen personenbezogenen Daten einzuschränken. Daher ist es möglich, dass auch besondere Kategorien personenbezogener Daten verarbeitet werden.
6. Datenquellen	Die primäre Datenquelle für die im Register gespeicherten Informationen ist der Meldende selbst, d.h. die Hinweisgebermeldung. Darüber hinaus kann es sich bei den Daten um Informationen handeln, die im Rahmen der Bearbeitung von Whistleblowing-Meldungen gespeichert wurden, wie z. B. Informationen, die von potenziell nahestehenden Personen erhalten wurden, und Informationen aus IT-Systemen.
7. Weitergabe von Daten und Offenbarung von Daten, Datenübermittlungen außerhalb des EU-/EWR-Raums	Die Identität des Meldenden wird, wenn sie bekannt ist, den Personen, gegen die sich die Ansprüche richten, nicht offengelegt. Die Identität des Hinweisgebers wird nur offengelegt, wenn der Hinweisgeber dies genehmigt hat oder wenn dies in einem Strafverfahren erforderlich ist. Personenbezogene Daten werden nur dann an Dritte, wie z.B. Behörden oder externe Prüfer, weitergegeben, wenn dies erforderlich ist. Der Systemanbieter des von Aidian genutzten Whistleblowing-Kanals ist die Juuriharja Consulting Group Oy und ihr Unterauftragsverarbeiter Gofore Oy, die in Not- oder Fehlersituationen, in denen technischer Support erforderlich ist, Zugang zu Informationen haben können. Der Hinweisgeberkanal ist als Cloud-Service implementiert und die Daten werden im EU/EWR-Raum gespeichert.

	Personenbezogene Daten werden grundsätzlich nicht außerhalb der EU oder des EWR übermittelt. In Ausnahmesituationen erfolgt die Datenübermittlung außerhalb des EWR unter Verwendung der Standardvertragsklauseln der Kommission und unter Umsetzung anderer geeigneter Schutzmaßnahmen (z. B. wenn die Daten verschlüsselt vorliegen). Auch direkte Identifikatoren wie Name oder Kontaktinformationen werden nicht hauptsächlich erhoben (es sei denn, der Meldende entscheidet sich im Zusammenhang mit der Meldung, diese selbst anzugeben).
8. Aufbewahrungsfrist für personenbezogene Daten	Der Bericht und alle Belege werden für 5 Jahre ab Erhalt des Berichts aufbewahrt, es sei denn, es sind weitere Maßnahmen im Wesentlichen mit der Angelegenheit im Gange oder eine längere Aufbewahrung ist erforderlich, um einen Rechtsanspruch vorzubereiten, geltend zu machen oder zu verteidigen. Wenn einige personenbezogene Daten für die Bearbeitung der Meldung oder anderweitig im Untersuchungsprozess nicht erforderlich sind, werden sie unverzüglich früher aus dem Untersuchungsmaterial entfernt.
9. Grundsätze der Sicherheitsmaßnahmen des Registers	Aidian hat geeignete technische und organisatorische Maßnahmen ergriffen, um personenbezogene Daten vor versehentlichem oder unrechtmäßigem Verlust, Offenlegung, Missbrauch, Änderung, Zerstörung oder unbefugtem Zugriff zu schützen. Die personenbezogenen Daten im Hinweisgeberkanal und im Untersuchungsprozess werden vertraulich und nur in einer dafür vorgesehenen sicheren Umgebung behandelt. Auf personenbezogene Daten können nur diejenigen benannten unabhängigen Mitglieder des Whistleblow-Teams zugreifen, die die Informationen benötigen, um die Untersuchung durchzuführen oder mögliche Sanktionen zu verhängen. <u>Grundsätze des Schutzes von Whistleblowing-Kanälen:</u> Der Hinweisgeberkanal ist durch technische Mittel (Verschlüsselungstechniken, Firewalls) geschützt. Der Whistleblowing-Kanal speichert keine IP-Adressen oder andere Informationen, die den Meldenden der Meldung identifizieren könnten. Die Informationssicherheit des Hinweisgeberkanals wurde von einem externen Prüfer überprüft und entspricht den an ihn gestellten regulatorischen Anforderungen. Die Daten im System werden regelmäßig gesichert. Das System speichert keine Informationen über den Meldenden, die er nicht selbst dort meldet. Während der Berichtsphase erhält der Meldende einen Zahlencode, mit dem er sich anmelden und die Bearbeitung der Meldung nach der Meldung überwachen kann. Dieser Zahlencode, der bei der Erstellung des Berichts angegeben wird, ist die einzige Möglichkeit, im Nachhinein auf den Bericht zuzugreifen. Aus diesem Grund sollte der Meldende den Zahlencode für sich selbst speichern, da dieser eindeutige Zahlencode die einzige Möglichkeit ist, die Bearbeitung der Meldung zu überwachen oder zusätzliche Informationen zur Meldung bereitzustellen. Wenn der Nummerncode vergessen wird, muss der Meldende eine neue Meldung vornehmen. Nur unabhängige, von Aidian speziell benannte Personen sind berechtigt, Meldungen zu bearbeiten, die über den Meldekanal eingehen.
10. Rechte der betroffenen Person	Die Rechte der betroffenen Person variieren je nach Rechtsgrundlage der Verarbeitung.

	Die betroffene Person kann die unten genannten Rechte ausüben, indem sie sich unter den in Abschnitt 2 genannten Kontaktdaten an den für die Verarbeitung Verantwortlichen wendet, vorzugsweise per E-Mail. <u>Wenn die Rechtsgrundlage für die Verarbeitung eine gesetzliche Verpflichtung ist, hat die betroffene Person die folgenden Rechte:</u> • Das Recht, Informationen über die Verarbeitung personenbezogener Daten zu erhalten. • Das Recht auf Zugang zu personenbezogenen Daten. ○ Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden. Die betroffene Person hat auch das Recht, Zugang zu den sie betreffenden personenbezogenen Daten und zu Informationen über die Verarbeitung ihrer personenbezogenen Daten zu erhalten. • Das Recht auf Berichtigung von Daten. ○ Die betroffene Person hat das Recht, dass sie betreffende unrichtige und unrichtige personenbezogene Daten unverzüglich berichtigt und unvollständige personenbezogene Daten vervollständigt werden. • Das Recht auf Einschränkung der Verarbeitung. ○ In bestimmten Situationen hat die betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen die Einschränkung der Verarbeitung zu verlangen. • Die betroffene Person hat das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung wie Profiling beruht und die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. • Das Recht, eine Beschwerde bei der Aufsichtsbehörde einzureichen. ○ Die betroffene Person hat das Recht, sich bei den Aufsichtsbehörden zu beschweren, wenn sie der Ansicht ist, dass ihre Rechte im Hinblick auf die EU-Datenschutzgrundverordnung verletzt worden sind: Büro des Datenschutzbeauftragten www.tietosuoja.fi/yhteystiedot Besuchsadresse: Lintulahdenkuja 4, 00530 Helsinki Postanschrift: PL 800, 00531 Helsinki Telefonzentrale.: 029 566 6700 Registernummer: 029 566 6768 E-Mail (Registrierung): tietosuoja(at)om.fi
--	---