SALUS
SEGUROS DE SALUD

ERWEITERTE INFORMATIONEN ÜBER DAS INTERNE INFORMATIONSSYSTEM (IIS) VON SALUS ASISTENCIA SANITARIA, S.A. DE SEGUROS

Im Rahmen der gesetzlichen Forderungen des Gesetzes 2/2023 vom 20. Februar 2023 über den Schutz persönlicher Daten, die Gesetzesverletzungen melden und sich am Kampf gegen Korruption beteiligen, wurde ein Rahmen geschaffen, der im von der Gesellschaft geschaffenen internen Informationssystem definiert ist.

Internes Informationssystem (IIS)

Definition	*Integrierter Rahmen*, der im internen Informationskanal und dem Verfahren zu internen Bearbeitung von Informationen, die in den Verantwortungsbereich des IIS fallen.
Zweck	Es wird als bevorzugter Kanal eingesetzt, um über Aktionen oder Unterlassungen entsprechend Artikel 2 zu informieren und gleichzeitig den Vertretern eine Reihe von Garantien zu bieten.
Ziel	Einrichtung eines entsprechenden Rahmens und Maßnahmen für die Implementierung eines IIS, das alle gesetzlichen Garantien erfüllt und Entwicklung eines Verfahrens zur Bearbeitung der erhalten Informationen bietet.
Sachlicher Anwendungsbereich	Es gilt für physische Personen, die über das von der Gesellschaft festgelegte Verfahren über Vorkommnisse in den folgenden Kategorien melden: • Alle Aktionen und Unterlassungen, die Gesetzesbrüche des Rechts der Europäischen Union darstellen können. • Aktionen und Unterlassungen, die schwere oder sehr schwere Verstöße gegen das Straf- oder Verwaltungsrecht darstellen können. Darunter versteht man alle schweren oder sehr schweren strafrechtlichen oder verwaltungsrechtlichen Verstöße, die einen wirtschaftlichen Schaden für die Steuerverwaltung und Sozialversicherung darstellen. • Alle Aktionen oder Unterlassungen, die sich aus den geltenden internen Regelungen der Gesellschaft ergeben.
Persönliches Umfeld	Es umfasst die folgenden Informantenkategorien: • *Gesellschafter und Vorstand von SALUS.* • Angestellte von SALUS (dazu gehören auch Praktikanten oder Personen in Ausbildung). • Personen, die kein Verhältnis mehr mit der Gesellschaft haben (das kann ein Arbeitsverhältnis, gewerbliches Verhältnis oder jegliches andere beendete Verhältnis sein.).

	• Gewerbliches Personal, das direkt mit den Aktivitäten der Gesellschaft in Verbindung steht. Medizinische Lieferanten, Vermittler, nicht medizinische Lieferanten. • Informanten, deren Arbeitsverhältnis oder gewerbliches Verhältnis noch nicht begonnen hat, wenn sich der Verstoß während des Auswahl- oder Verhandlungsverfahrens ergeben sollte. • Versicherte von SALUS. • Jegliches andere Interessensgruppen, die, auch wenn sie nicht spezifisch im vorliegenden Ethik- und Verhaltenskodex genannt worden sind, eine direkte Verknüpfung mit den von der Gesellschaft geleisteten Diensten stehen. • (Physische oder juristische) Personen, die direkt oder indirekt am Kommunikationsverfahren teilnehmen.

Aufbau des IIS

Interner Informationskanal	Einziger Kommunikationsweg für den Erhalt von Informationen, die den sachlichen Anwendungsbereich dieser Politik verletzen können.
Internes Bearbeitungsverfahren für Informationen	Dieses wird mit dem Zweck eingerichtet, die Informationen mit Effektivität und den erforderlichen Garantien zu bearbeiten. Es wird in einem speziellen Verfahren beschrieben.

Rollen im IIS

Verantwortliche Person im System	Die Gesellschaft ist die verantwortliche Person für die Einrichtung des internen Informationssystems (IIS) und ist auch die verantwortliche Person für die Bearbeiten der persönlichen Daten im Rahmen der geltenden Regelungen zum Schutz persönlicher Daten.
Verantwortliche Person der Verwaltung	Der Verwaltungsrat von SALUS hat als verantwortliche Person des IIS die verantwortliche Person für die Einhaltung der geltenden Regelungen (RCN) benannt. Diese Berufung wurde der Behörde für die unabhängige Informationen mitgeteilt.

Eigenschaften und Grundsätze des IIS

Eigenschaften und	Es ermöglicht die Kommunikation über die oben aufgeführten Verstoßkategorien.
	Es wurde mit Sicherheit entworfen und betrieben.

Grundsätze des IIS	Es verhindert dem Personal den unbefugten Zugriff.
	Es erlaubt die Vorlage schriftlicher, verbaler oder beider Kommunikationsarten.
	Es beinhaltet alle internen Kanäle, die in der Gesellschaft existieren können.
	Mit einem Verfahren wird eine Effektivität der Bearbeitung der erhaltenen Kommunikationen mit dem Anliegen ermöglicht, der erste zu sein, der über eine mögliche Unregelmäßigkeit erfährt, die gemeldet wird.
	Das Bearbeitungsverfahren bietet die nötigen Informationen zum Schutz des Informationen unter Berücksichtigung der Ausführungen in Artikel 9.
	Es verfügt über ein nicht öffentliches Registersystem der erhaltenen Meldungen, um die vom Gesetz geforderte Vertraulichkeit zu garantieren.

Schutz persönlicher Daten

Juristischer Rahmen der Bearbeitung	Die Bearbeitung persönlicher Daten richtet sich nach den Ausführungen der EU-Richtlinie 2016/679, dem Organischen Gesetz 3/2018 und besonders auf Titel VI des Gesetzes 2/2023.
Zulässigkeit	Als *zulässig* werden alle Verfahren zum Schutz persönlicher Daten angesehen, die zur Anwendung des Gesetzes 2/2023 notwendig sind, wobei die Gesellschaft zur Einrichtung eines IIS verpflichtet ist.
Beschränkung der Bearbeitung	Der Zugriff wird ausschließlich auf die im System definierten Beteiligten beschränkt.
Garantien im System:	Das Werkzeug, das den internen Informationskanal betreibt, verfügt über alle technischen Maßnahmen zur Bewahrung der Vertraulichkeit der betroffenen Personen und Schutz deren Identität.

Maßnahmen zum Schutz von Informanten und betroffenen Personen

Bedingungen zum Schutz von Informanten und betroffenen Personen	Prinzip zum Schutz des Informanten unter der Voraussetzung, dass dieser angemessene Gründe hatte, dass die Informationen wahr seinen und es unter die Anwendung des vorliegenden Gesetzes fällt und alle Schutzgarantien geboten werden, die der Fall erfordert.
	Dies wird auf die betroffenen Personen, den Schutz deren Identität und Garantie der Vertraulichkeit der Taten und Daten des Verfahrens ausgeweitet.
Verbot von Repressalien	Repressalien (Taten, Drohungen und Versuche) gegen die Personen, die eine Kommunikation vorlegen, werden ausdrücklich verboten. Als Repressalie wird verstanden:

	Jegliche Aktion oder Unterlassung, die vom Gesetz verboten ist oder die direkt oder indirekt eine nachteilige Behandlung bedeutet, die die Personen, die besonders unter diesem Nachteil in Bezug auf andere im Arbeits- oder Berufsumfeld nur durch ihre Rolle als Informant oder nach einer öffentlichen Aufdeckung darunter leiden.
	Unter Repressalien versteht man enuntiativ: ● Suspendieren des Arbeitsvertrags, Kündigung oder Vertragsauflösung, Verweigerung der Verlängerung, es sei denn, sie werden all reguläre Ausübung der Geschäftsleitung und unter Einhaltung der Arbeitsgesetzgebung ausgesprochen. ● Schäden, inklusive Rufschädigungen, wirtschaftliche Verluste, Nötigung, Einschüchterungen, Schikanen oder Verfemung ● Negativen Referenzen, die mit der Ausübung zu tun haben. ● Eintrag in Schwarze Listen ● Verweigerung oder Entzug von Zulassungen/Lizenzen ● Verweigerung von Ausbildungen ● Diskriminierung oder nachteilhafte oder ungerechte Behandlung

SALUS
SEGUROS DE SALUD

+ NUZTER DES INTERNEN INFORMATIONSSYSTEMS

Mit welchem Zweck verarbeiten wir die persönlichen Daten, die uns zur Verfügung gestellt werden?

Verarbeitung der Informationen, die im INTERNEN INFORMATIONSSYSTEM bearbeitet werden.

Empfänger der Kommunikation ist die Verantwortliche Person im System von SALUS ASISTENCIA SANITARIA, S.A. DE SEGUROS, die die Privatsphäre der Personen, die die Anwendung nutzen, auf größtmögliche Weise schützt und ihre persönlichen Daten mit Schutz und vertraulich verarbeitet. Dazu informiert sie die Nutzer darüber, dass:

in Erfüllung der Regelungen zum Schutz persönlicher Daten und Gesetzen zum Schutz der anzeigenden Person, deren Daten und die gelieferten Informationen (und die Daten anderen Personen, die zur Verfügung gestellt wurden) zu den spezifischen Zwecken verarbeitet, die die vorliegende Datenschutzrichtlinie vorsieht.
keine automatischen Entscheidungen getroffen oder Profile in Bezug auf die gesammelten Informationen und Daten erstellt werden.

Welche gesetzliche Grundlage hat die Verarbeitung ihrer Daten?
Die Verarbeitung persönlicher Daten im Fall von interner Kommunikation wird als legal unter den Ausführungen der Artikel 6.1c) der EU-Richtlinie 2016/679 des Europäischen Parlaments und des Rats vom 27. April 2016, 8 des Organischen Gesetzes 3/2018 vom 5. Dezember und 11 des Organischen Gesetzes 7/2021 vom 26. Mai erachtet, sofern es entsprechend den Ausführungen der Artikel 10 und 13 der vorliegenden Gesetze notwendig ist, über ein internes Informationssystem zu verfügen.
Wenn dies nicht vorgeschrieben ist, richtet sich die Bearbeitung nach Artikel 6.1e der erwähnten Richtlinie.
Die Verarbeitung persönlicher Daten im Fall von interner Kommunikation wird als legal unter den Ausführungen der Artikel 6.1c) der EU-Richtlinie 2016/679 des Europäischen Parlaments und des Rats vom, 8 des Organischen Gesetzes 3/2018 vom 5. Dezember und 11 des Organischen Gesetzes 7/2021 vom 26. Mai erachtet.

Wie lange werden die gelieferten Daten gespeichert?

Die Daten in der Meldung und der betroffenen Personen und Dritter werden im System nur während der Zeit gespeichert, die notwendig ist, um über einen Beginn einer Untersuchung über die Vorfälle zu beginnen. Auf jeden Fall werden 3 Monate nach der Eingabe der Daten diese im System gelöscht, sofern die Aufbewahrung nicht als Beweis für den Nachweis der Vorbeugung der Kommission für Straftaten durch die juristische Person entsprechend der Ausführungen des Artikels 24 des Organischen Gesetzes 3/2018 vom 5. Dezember über den Schutz persönlicher Daten und Bewahrung digitaler Rechte (im folgenden Text LOPDGDD genannt) erforderlich ist

Auf keinen Fall werden die persönlichen Daten, die nicht für die Erkenntnisse und Untersuchung der Information, notwendig sind verarbeitet und werden selbst unmittelbar gelöscht. Ebenso werden alle persönlichen Daten gelöscht, die kommuniziert worden sind und sich auf Verhaltensweisen beziehen, die nicht unter den Rahmen des Gesetzes 2/2023 fallen.

Wenn sich die zur Verfügung gestellten Informationen als nicht wahrheitsgemäß herausstellen, werden diese in dem Moment gelöscht, an dem dieser Umstand bekannt wird, es sei denn, dass dieser Umstand ein strafrechtliches Vergehen darstellt und die Informationen in diesem Fall so lange gespeichert werden, wie es für das Gerichtsverfahren notwendig ist.

Welche Empfänger dürfen ihre Daten erhalten?

Organisationen oder Personen, die direkt vom der verantwortlichen Person für die Verarbeitung für die Leistung von Aufgaben zu tun haben, die mit den Zwecken der Verarbeitung in Verbindung stehen. Mitarbeiter und Unterlieferanten für die Verwaltung des Ethikkanals, Berater und Auditoren des Systems zur gesetzlichen Erfüllung der Organisation.

Der Zugriff auf die persönlichen Daten im internen Informationssystem ist beschränkt auf (i) die verantwortliche Person des internen Informationssystems und der Person, die direkt als systemverantwortliche Person agiert*, (ii) die verantwortliche Person der Personalabteilung, wenn disziplinarische Maßnahmen ergriffen werden, (iii) die verantwortliche Person der Gerichtsbarkeit (wenn man gesetzliche Maßnahmen mit

den gemeldeten Taten ergreifen müsste), (iv) die verantwortlichen Personen für die Verarbeitung, die man möglicherweise benennt und (v) den Datenschutzbeauftragten.
Sicherheitskräfte und Strafverfolgungsbehörden: abhängig davon, ob sie ein gerechtfertigtes Recht auf Zugriff im Rahmen der Untersuchung eines Regelverstoßes haben. Die Verarbeitung von Daten durch andere Personen oder sogar in Kommunikationen an Dritte, sofern es für die Verarbeitung der Sanktions- oder Strafmaßnahmen nötig ist, die sich daraus ergeben könnten, ist legal. Die Identität der informierenden Person darf nur an die Strafverfolgungsbehörden, das Finanzministerium oder die für die strafrechtliche, disziplinarische oder die Bußmaßnahme zuständige Behörde gemeldet werden. Die Enthüllungen in diesem Bereich unterliegen den in den geltenden Gesetzen festgelegten Regelungen. Die informierende Person wird versetzt, bevor seine Identität bekanntgegeben wird, es sei denn, diese Information könnte die juristische Untersuchung oder Verfolgung beeinträchtigen.

Unter welchen Garantien werden die Daten kommuniziert?

Die Akzeptierung der vorliegenden Bedingungen impliziert die Sammlung persönlicher Daten, die Nutzer im Ethikkanal eingeben und ihr unmissverständliches Einverständnis, dass SALUS ASISTENCIA SANITARIA, S.A. DE SEGUROS diese für die Verarbeitung der Anzeigen und/oder Informationen (Kommunikationen) verarbeitet, wobei der Empfänger der in ihnen geschilderten Taten die verantwortliche Person im System von SALUS ASISTENCIA SANITARIA, S.A DE SEGUROS ist.
Mit der Akzeptierung dieser Politik bestätigen die Personen, dass die zur Verfügung gestellten Daten wahr, bestätigt, vollständig und aktuell sind und dass sie jegliche Änderungen umgehend mitteilen.
Ebenso erklärt die Person mit der Akzeptierung und/oder Prüfung des Verfahrens zur Verarbeitung der Kommunikation über das Formular im System, dass sie älter als 14 Jahre, juristisch handlungsfähig ist und ausdrücklich der Verarbeitung der Daten entsprechend den Festlegungen in der Zusatzklausel und den Zusatzinformationen über Datenschutz zustimmt. Bei Fällen, die ein Minderjähriger unter 14 Jahren oder eine Person ohne juristische Handlungsfähigkeit vorlegen, erklärt der Erziehungsberechtigte, Vormund oder zuständige gesetzliche Vertretung des/der Minderjährigen, dass deren Begründung von den Verantwortlichen der Verarbeitung notwendig sein kann, um eine akzeptierte Einverständniserklärung zu erhalten.

Alle Nutzer müssen wissen, dass die Kommunikationen vertraulich und eingeschränkt behandelt werden. Dazu wird besonders die Identität der aus guten Glauben meldenden Personen geschützt, die vor jeglichen Repressalien geschützt werden, die diese Meldung nach sich ziehen könnte.

Die verantwortliche Person im internen Informationssystem veröffentlicht zu keinem Zeitpunkt die Daten der Person, die die Kommunikation geschickt hat und im Formular auf der Internetseite eingegeben wurde, es sei denn, dass:

dies juristisch nötig oder von der zuständigen Behörde verlangt wird.

die verantwortliche Person des internen Informationssystems im Hinblick auf die Meldung und aus begründetem Anlass es für unbedingt notwendig erachtet, unter der Voraussetzung, dass die meldende Person ihr ausdrückliches Einverständnis dazu erteilt.

objektive Gründe vorliegen, die zur Annahme führen, dass die Meldung aus vorsätzlichem Verhalten (z. B. auf Basis falscher Dokumente) abgeschickt worden ist und die verantwortliche Person im im internen Informationssystem die Identität der meldenden Person weitergibt, um ausschließlich die disziplinarischen Maßnahmen zu ergreifen.

Es wird alle Nutzern empfohlen, niemandem den Benutzernamen, das Passwort und die alphanumerische Referenz der Kommunikation mitzuteilen. Die Kommunikation von Daten, die von Dritten und/oder verantwortlichen Personen für die Bearbeitung durchgeführt werden, wird von Körpern durchgeführt, die ein System zum Schutz persönlicher Daten entsprechend der geltenden Gesetze besitzen.