

Das Institut des „Whistleblowing“ beim Land und einigen seiner abhängigen Körperschaften

Audit gemäß Artikel 50 Absatz 1 Buchstabe e) des Landesgesetzes Nr. 6/2022



AUDITORS

Cinzia Flaim

Irmgard Prader

Übersetzung: Übersetzungsamt des Südtiroler Landtages

PRÜFSTELLE

ORGANISMO DI VALUTAZIONE

39100 Bozen | Freiheitsstraße 66
39100 Bolzano | Corso Libertà, 66

Tel. 0471 402 212 | Fax 0471 260 114
pruefstelle@landtag-bz.org | organismodivalutazione@consiglio-bz.org
www.landtag-bz.org/de/pruefstelle.asp
www.consiglio-bz.org/it/organismo-di-valutazione.asp
PEC: pruefstelle.organismovalutazione@pec.prov-bz.org

Dezember 2024

INHALTSVERZEICHNIS

I.	Einführung	
1.1	Ziel, Gegenstand und Methodik des Audits	4
1.2	Rechtlicher Bezugsrahmen	5
II.	Analyse des Ist-Zustands	
2.1	Whistleblowing in der Landesverwaltung	15
2.2	Whistleblowing in der Agentur für Energie Südtirol – KlimaHaus.....	20
2.3	Whistleblowing im Institut für den sozialen Wohnbau (WOBI).....	22
III.	Schlussfolgerungen	
3.1	Die Südtiroler Landesverwaltung	23
3.2	Agentur für Energie Südtirol – KlimaHaus.....	24
3.3	Das Institut für den sozialen Wohnbau (WOBI) der Autonomen Provinz Bozen ...	25

I. Einführung

1.1 Ziel, Gegenstand und Methodik des Audits

Laut Artikel 50 Absatz 1 Buchstabe e) des Landesgesetzes Nr. 6/2022 verfasst die Prüfstelle einen Bericht über die Gesetzmäßigkeit, die Unparteilichkeit und die reibungslose Abwicklung der Verwaltungstätigkeit des Landes und der von ihm abhängigen Körperschaften.

Das Tätigkeitsprogramm der Prüfstelle beinhaltet für das Jahr 2024 im Bereich der genannten Kontrolltätigkeiten die Fortsetzung des Audits, das bereits 2023 eingeleitet wurde und die Umsetzung des Whistleblowings beim Land und einigen seiner abhängigen Körperschaften zum Inhalt hat. Dabei handelt es sich um ein Institut zum Schutz jener Bediensteten, die unrechtmäßige oder nicht ordnungsgemäße Vorgänge am Arbeitsplatz den zuständigen Stellen melden, sodass diese eingreifen können.

Dies stellt einen wichtigen Baustein für die Einhaltung der Regeln und der ethischen Prinzipien im öffentlichen Bereich dar, der in der europäischen und nationalen Gesetzgebung als Institut zur Vorbeugung gegen rechtswidrige Vorgehensweisen und gleichzeitig als Ausdruck des Rechts des Einzelnen auf Meinungsäußerung geregelt ist.

Im Rahmen des Audits wurden folgende Aspekte untersucht:

- rechtlicher Bezugsrahmen gemäß Richtlinie (EU) 2019/1937 und Gesetzesvertretendem Dekret Nr. 24/2023 sowie Rechtsrahmen der Autonome Provinz Bozen, in denen das Institut des Whistleblowings geregelt ist;
- Aktivierung der Meldekanäle und der Verfahren zur Bearbeitung der Meldungen;
- organisatorische Maßnahmen zur Geheimhaltung der Identität und zum Schutz vor etwaigen Repressalien;
- Schulung des Personals für die Annahme der Meldungen.

Diese Aspekte wurden mit Bezug auf das Land und zwei seiner abhängigen Körperschaften festgelegt; aufgrund der professionellen Bewertung der Auditoren wurden zwei Einrichtungen ausgewählt, die seit längerer Zeit keinem Audit unterzogen worden waren, nämlich das Institut für den sozialen Wohnbau des Landes Südtirol und die Agentur für Energie Südtirol – KlimaHaus;

In Bezug auf die bereits erwähnten Aspekte bestand das Ziel des Audits darin, zu überprüfen, ob beim Land, im Wohnbauinstitut und bei der Agentur für Energie Südtirol – KlimaHaus das Whistleblowing umgesetzt wurde und dabei die entsprechenden Gesetzesvorgaben eingehalten wurden.

Das Audit erfolgte gemäß den Leitlinien für Audit- und Beratungstätigkeiten, die von der Prüfstelle am 20. Januar 2021 genehmigt wurden und ihrerseits auf den beruflichen Standards des IIA (Institute of Internal Auditors) sowie den Prüfungsnormen der INTOSAI (International Organisation of Supreme

Audit Institutions) fußen. Dazu wurde der Direktor des Landesamtes für institutionelle Angelegenheiten und der Mitarbeiter dieses Amtes, der sich mit der Bearbeitung von Meldungen befasst, befragt. Dabei ging es auch um eine Demo zur neuen digitalen Plattform für die Meldungen. Zudem wurden dem Direktor des Instituts für den sozialen Wohnbau des Landes Südtirol und jenem der Agentur für Energie Südtirol – KlimaHaus ein Fragebogen übermittelt.

1.2 Rechtlicher Bezugsrahmen

Das Institut des Whistleblowings wurde im italienischen Recht zum ersten Mal mit dem Gesetz Nr. 190/2021 eingeführt, mit dem das gesetzvertretende Dekret Nr. 165 vom 30. März 2001 abgeändert und der Artikel 54-bis eingeführt wurde. In dieser Bestimmung wurde ein Schutzmechanismus für jene öffentlichen Bediensteten vorgesehen, die auf ein ordnungswidriges Vorgehen innerhalb der Einrichtung, in der sie arbeiten, hinweisen.

Infolge des Inkrafttretens der EU-Richtlinie Nr. 1937 vom 23. Oktober 2019 des Europäischen Parlaments und des Rates betreffend den „*Schutz von Personen, die Verstöße gegen das Unionsrecht melden*“ samt Bestimmungen zum Schutz von Personen, die Verstöße gegen nationale Rechtsnormen melden, sowie des gesetzvertretenden Dekrets Nr. 24 vom 10. März 2023 betreffend die Umsetzung der Richtlinie (EU) 2019/1937 des Europäischen Parlamentes und des Rates wird eine detaillierte und allumfassende Regelung erlassen, die auch für den Privatsektor gilt und darauf abzielt,

- die Whistleblower zu schützen, also jene Personen, die im Rahmen einer Arbeitstätigkeit im öffentlichen oder privaten Bereich Verstöße gegen nationale oder EU-Bestimmungen zum Schaden des öffentlichen Interesses oder der Integrität der öffentlichen Verwaltung oder einer privaten Einrichtung feststellen und diese bei den Gerichts- oder Rechnungsführungsbehörden, melden, offenlegen oder anzeigen;
- mit abschreckenden und vorbeugenden Maßnahmen rechtswidrige Handlungen und Missstände in der Verwaltung zu verhindern und die Transparenz und Rechenschaftspflicht in öffentlichen und privaten Einrichtungen zu stärken, um, wie in der genannten europäischen Richtlinie festgelegt wurde, zu „einer Kultur der guten Kommunikation und der sozialen Verantwortung von Unternehmen beizutragen, in deren Rahmen Hinweisgeber als Personen gelten, die wesentlich zu Selbstverbesserung und herausragender Kompetenz innerhalb der Organisation beitragen“.

Auf Landesebene gelten die nationalen Bestimmungen weiterhin als rechtlicher Bezugsrahmen für den Schutz der Whistleblower; die entsprechende Umsetzung erfolgt derzeit durch den Beschluss der Landesregierung Nr. 94 vom 06.02.2018, in dem die Vorgehensweise für die Bearbeitung von Meldungen von unrechtmäßigen Handlungen geregelt wurde.

Im Folgenden seien die Kernpunkte der nationalen Bestimmungen angeführt.

1.2.1 Zielgruppe der Bestimmungen zum Schutz der Whistleblower

Zur Zielgruppe der Bestimmungen zum Schutz der Whistleblower gehören nicht nur Angestellte, sondern ein breites Spektrum an Personengruppen, die zwar nicht als Arbeitnehmer eingestuft

werden können, sich jedoch im Rahmen einer beruflichen Tätigkeit in einer wirtschaftlich prekären Lage befinden können (Vgl. Art. 3 des Gesetzesvertretenden Dekrets Nr. 24/2023). Dazu zählen:

- Selbstständige, die ihre berufliche Tätigkeit bei Einrichtungen des öffentlichen oder des privaten Sektors ausüben;
- Mitarbeiter, Freiberufler und Berater, die ihre Tätigkeit bei Einrichtungen des öffentlichen oder des privaten Sektors ausüben;
- Freiwillige und Praktikanten, mit und ohne Entlohnung;
- Aktionäre und Personen mit Verwaltungs-, Führungs-, Kontroll-, Aufsichts- oder Vertretungsfunktionen in Einrichtungen des öffentlichen oder privaten Sektors, auch falls diese Funktionen lediglich de facto ausgeübt werden.

Die Bestimmungen zum Schutze der Hinweisgeber gelten auch für:

- all jene, die im selben beruflichen Kontext tätig sind und die Whistleblower beim Meldeverfahren unterstützen (die sogenannten „Mittler“);
- Personen im selben beruflichen Kontext des Hinweisgebers, oder jene, bei denen eine stabiles Näheverhältnis oder eine Verwandtschaft bis zum vierten Grad zu einer Person, die Anzeige erstattet oder eine Offenlegung vorgenommen hat, besteht;
- Arbeitskollegen des Hinweisgebers oder der Person, die Anzeige erstattet oder eine Offenlegung vorgenommen hat, wenn sie im selben Arbeitsumfeld wie diese Person tätig sind und regelmäßig und dauerhaft mit dieser Person in Kontakt sind.

Die Meldung kann nicht nur während des bestehenden Arbeitsverhältnisses oder während der Dauer einer Mitarbeit erfolgen, sondern auch in folgenden Fällen:

- wenn noch kein Rechtsverhältnis besteht, die Informationen über die Verstöße während des Auswahlverfahrens oder in anderen vorvertraglichen Phasen erlangt wurden;
- während der Probezeit;
- nach Auflösung des Rechtsverhältnisses, wenn die Informationen über die Verstöße vor Auflösung des Verhältnisses erlangt wurden (Pensionisten).

1.2.2 Gegenstand der Meldung des Whistleblowers

Gegenstand von Meldungen, Offenlegungen oder Anzeigen können Verstöße gegen nationale oder EU-Bestimmungen sein, die dem öffentlichen Interesse oder der Integrität der öffentlichen Verwaltung oder einer privaten Einrichtung schaden und die in einem öffentlichen oder privaten Arbeitsumfeld festgestellt wurden (vgl. Art. 2 des Gesetzesvertretenden Dekrets Nr. 24/2023).

Dabei handelt es sich also um Informationen über Verhaltensweisen, Handlungen oder Unterlassungen, die dem öffentlichen Interesse oder der Integrität der öffentlichen Verwaltung oder einer privaten Einrichtung schaden, darunter beispielsweise folgende:

- verwaltungsrechtliche, buchhalterische, zivil- oder strafrechtliche Verstöße oder rechtswidrige Handlungen gemäß dem Gesetzesvertretenden Dekret Nr. 231 vom 8. Juni 2001 oder Verstöße gegen die darin vorgesehenen Organisations- und Verwaltungsmodelle;
- Verstöße, die in den Geltungsbereich von Rechtsakten der Europäischen Union fallen (z. B. öffentliches Auftragswesen; Dienstleistungen, Finanzprodukte und -märkte sowie Vorbeugung gegen Geldwäsche; Produktsicherheit und -konformität; Verkehrssicherheit; Umweltschutz; Lebensmittel- und Futtermittelsicherheit sowie Tiergesundheit und Tierwohl; öffentliche Gesundheit; Verbraucherschutz; Schutz der Privatsphäre und Schutz personenbezogener Daten; Sicherheit von Netzwerken und Informationssystemen);
- Handlungen oder Unterlassungen, die gegen die finanziellen Interessen der Union gerichtet sind;
- Handlungen oder Unterlassungen, die den Binnenmarkt betreffen (z. B. Verstöße gegen die Wettbewerbsvorschriften oder im Bereich der staatlichen Beihilfen);
- Handlungen oder Unterlassungen, die dem Ziel oder dem Zweck der Vorschriften der Rechtsakte der Union zuwiderlaufen.

Die Informationen können nicht nur die genannten Verhaltensweisen, Handlungen oder Unterlassungen betreffen, sondern ebenso folgende:

- Verhaltensweisen zur Verschleierung der genannten Verstöße;
- rechtswidrige Handlungen, die noch nicht begangen wurden, von denen der Whistleblower aber vernünftigerweise glaubt, dass sie erfolgen könnten, wenn konkrete, präzise und übereinstimmende Hinweise vorliegen;
- begründete Verdachtsmomente in Bezug auf die genannten Verstöße.

Von den vorgesehenen Schutzbestimmungen ausgeschlossen sind ausschließlich jene Meldungen, Ansprüche oder Forderungen, die mit einem persönlichen Interesse der Hinweisgeber verbunden sind und ausschließlich das individuelle Arbeitsverhältnis oder das Beschäftigungsverhältnis im öffentlichen Sektor in Bezug auf hierarchisch höher eingestufte Personen betreffen.

1.2.3 Meldekanäle und -verfahren

Die verschiedenen Einrichtungen müssen einen eigenen internen Meldekanal für die Übermittlung und Bearbeitung der Meldungen einrichten (s. Art. 4 des Gesetzesvertretenden Dekrets Nr. 24/2023). Dabei muss Folgendes gewährleistet werden:

- Schutz der Vertraulichkeit, auch durch Verwendung von kryptographischen Elementen, falls IT-Instrumente verwendet werden;
- Möglichkeit der Meldungen in Schriftform, auch über EDV-gestützte Wege (Online-Plattform), oder in mündlicher Form, telefonisch oder alternativ dazu mittels Sprachnachrichten, oder aber, falls der Hinweisgeber dies wünscht, in einem persönlichen Treffen, das binnen einer angemessenen Frist stattfinden soll.

Die entsprechenden Einrichtungen müssen die Verfahren für die Annahme und Bearbeitung der Meldungen festlegen.

Öffentliche Einrichtungen, die zur Ernennung eines Verantwortlichen für Korruptionsvorbeugung und Transparenz verpflichtet sind, müssen diesen mit der Betreuung des internen Meldekanals beauftragen. Anschließend werden weitere Personen ausgewählt und ausdrücklich entsprechend ermächtigt, die sich unter der Leitung des Verantwortlichen für Korruptionsvorbeugung und Transparenz mit der Annahme und Bearbeitung der Meldungen befassen.

Um eine effiziente und zeitnahe Bearbeitung der Meldungen sowie angemessene Folgemaßnahmen zu gewährleisten, wurden in den Bestimmungen die Verfahrensweisen nach Eintreffen einer internen Meldung geregelt (s. Art. 5 des Gesetzesvertretenden Dekrets Nr. 24/2023), an die sich die mit der Bearbeitung der Meldungen Betrauten halten müssen; diese sind dazu verpflichtet:

- innerhalb einer Frist von sieben Tagen nach Eingang der Meldung an den Hinweisgeber eine Bestätigung dieses Eingangs zu richten;
- mit dem Hinweisgeber in Kontakt zu bleiben;
- bei Bedarf Ergänzungen einzufordern;
- dem Hinweisgeber binnen drei Monaten ab Eingang der Meldung eine Rückmeldung zu übermitteln.

Die verschiedenen Einrichtungen sind zudem dazu verpflichtet (s. Art. 5 des Gesetzesvertretenden Dekrets Nr. 24/2023), auf ihren Internetseiten klare Informationen und in jedem Fall leicht zugängliche Informationen zur Nutzung des Meldekanals zur Verfügung zu stellen, um Fehlern seitens des Hinweisgebers vorzubeugen.

Dem Whistleblower steht auch ein externer Meldekanal zur Verfügung, mit dem die Antikorruptionsbehörde (ANAC) betraut ist und ausschließlich unter folgenden, im Gesetzesvertretenden Dekret Nr. 24/2023 (s. Art. 7) ausdrücklich und zwingend vorgesehenen Bedingungen verwendet werden kann:

- a) der interne Meldekanal ist nicht aktiv oder er ist zwar aktiv, entspricht aber nicht den Bestimmungen;
- b) der Hinweisgeber hat bereits eine interne Meldung übermittelt, es wurden jedoch keine Folgemaßnahmen ergriffen;
- c) der Hinweisgeber hat berechtigte Gründe zur Annahme, dass einer internen Meldung nicht wirksam Folge geleistet würde oder dass diese Meldung Repressalien zur Folge haben könnte;
- d) der Hinweisgeber hat berechtigte Gründe zur Annahme, dass der Verstoß eine imminente oder offensichtliche Gefahr für das öffentliche Interesse birgt.

Es handelt sich um einen Mechanismus, mit welchem dem Whistleblower bei Bedarf zusätzliche Instrumente im Sinne einer Entschärfung der Situation zur Verfügung gestellt werden sollen. Auch zur Nutzung dieses Meldekanals sind die Einrichtungen dazu verpflichtet, klare Informationen zu übermitteln.

1.2.4 Der gute Glaube des Whistleblowers

Im genannten Gesetzesvertretenden Dekret ist ein Schutzmechanismus zugunsten des Whistleblowers vorgesehen, der unter der Voraussetzung einsetzt, dass dieser zum Zeitpunkt der Meldung berechnigte Gründe zur Annahme hat, dass die Informationen zu den gemeldeten Verstößen der Wahrheit entsprechen (vgl. Art. 16 des Gesetzesvertretenden Dekrets Nr. 24/2023).

Somit muss der gute Glaube des Hinweisgebers bestehen, gestützt von objektiven Sachverhalten, die beim Hinweisgeber zur berechtigten Überzeugung führen, dass die dargestellten Ereignisse der Wahrheit entsprechen (und nicht Gerüchten, offensichtlichen Fehlinformationen oder allgemein bekannten Tatsachen entstammen).¹ Die (möglicherweise auch persönlichen) Gründe, aus denen die betreffende Person beschlossen hat, Verstöße zu melden, sie zur Anzeige zu bringen oder offenzulegen, sind nicht von Belang. Allein die objektive Tragweite der gemeldeten Sachverhalte ist von Bedeutung.

Um das richtige Maß zu finden, muss nach Meinung der ANAC in jedem einzelnen Fall überprüft werden, ob der Gegenstand der Meldung durch den öffentlichen Bediensteten beim Hinweisgeber zur Überzeugung geführt hat, dass die Integrität der öffentlichen Verwaltung geschützt werden muss. Diese Überzeugung muss jedoch nicht der einzig bestehende Beweggrund sein; vielmehr kann parallel dazu auch ein persönliches Interesse des Hinweisgebers bestehen, das durch den Schutz des öffentlichen Interesses ebenfalls erfüllt würde.²

1.2.5 Der Schutzmechanismus

Der Schutzmechanismus gemäß dem genannten Dekret (vgl. Art. 12 und Teil II des Gesetzesvertretenden Dekrets Nr. 24/2023) gliedert sich in vier Formen des Schutzes:

1. Schutz der Vertraulichkeit;
2. Schutz vor Repressalien;
3. Haftungsbeschränkung;
4. Unterstützungsmaßnahmen.

Die ersten drei Formen betreffen die Bediensteten; die vierte hingegen betrifft die Möglichkeit für die ANAC, Abkommen mit Körperschaften des dritten Sektors abzuschließen, damit diese im Falle einer Meldung kostenlose Unterstützung und Beratung anbieten.

1.2.6 Schutz der Vertraulichkeit

Der Schutz der Vertraulichkeit (vgl. Artikel 3 des Gesetzesvertretenden Dekrets Nr. 24/2023) sieht Folgendes vor:

- Die Meldung und die dazugehörige Dokumentation sind von der Ausübung des Rechts auf

¹ Vgl. erläuternder Bericht zu den Leitlinien betreffend den Schutz von Personen, die Verstöße gegen das EU-Recht und gegen die nationalen Bestimmungen melden, genehmigt mit Beschluss der ANAC Nr. 311 vom 12. Juli 2023.

² Vgl. <https://www.anticorruzione.it/-/delibera-numero-311-del-21-giugno-2022>.

Zugang zu Dokumenten sowie von der Ausübung des Rechts auf Bürgerzugang ausgenommen;

- Es ist verboten, die Identität des Hinweisgebers anderen Personen als denjenigen, die für die Entgegennahme oder Weiterverfolgung von Meldungen zuständig und ausdrücklich zur Verarbeitung dieser Daten befugt sind, mitzuteilen. Der Gesetzgeber legt fest, dass nicht nur der Name des Hinweisgebers, sondern auch alle anderen Informationen, aus denen direkt oder indirekt die Identität der meldenden Person abgeleitet werden kann, geschützt werden müssen.

Das Verbot der Offenlegung gilt auch für die Person, an welche die Meldung gerichtet ist, sowie für die in der Meldung genannten Personen bis zum Abschluss des auf der Grundlage der Meldung eingeleiteten Verfahrens.

Schließlich darf im Disziplinarverfahren die Identität des Hinweisgebers nicht bekannt gegeben werden, wenn die Vorhaltung des zur Last gelegten Disziplinarvergehens auf Ermittlungen beruht, die zusätzlich und unabhängig von der Meldung erfolgt sind (auch wenn diese nach der Vorhaltung in die Wege geleitet werden). Die Meldung darf nur dann für die Zwecke eines Disziplinarverfahrens gegen die gemeldete Person verwendet werden, wenn:

- ein solches Verfahren sich ganz oder teilweise auf die Meldung stützt;
- die Kenntnis der Identität des Hinweisgebers für die Verteidigung des Beschuldigten unerlässlich ist;
- der Hinweisgeber, nachdem er schriftlich über die Gründe für die Offenlegung informiert wurde, in die Offenlegung seiner Identität eingewilligt hat.

Um das Recht auf Schutz der personenbezogenen Daten der Hinweisgeber oder der Personen, die Anzeige erstattet haben, zu gewährleisten, hat der Gesetzgeber vorgesehen, dass die Erfassung und Bearbeitung von Meldungen, öffentlichen Bekanntmachungen oder Beschwerden, einschließlich der Kommunikation zwischen den zuständigen Behörden, in Übereinstimmung mit den Rechtsvorschriften über den Schutz personenbezogener Daten zu erfolgen hat.³

Gemäß dem Gesetzesvertretenden Dekret Nr. 24/2023 sind die für die Datenverarbeitung Verantwortlichen jene Stellen, die die internen Meldewege einrichten (in unserem Fall die Autonome Provinz Bozen oder die einzelnen Einrichtungen).

Bekanntlich sehen die Vorschriften über den Schutz personenbezogener Daten vor, dass die für die Verarbeitung Verantwortlichen und die für die Verarbeitung Mitverantwortlichen unter ihrer eigenen Verantwortung und im Rahmen ihrer eigenen Organisationsstruktur dafür sorgen müssen, dass bestimmte Aufgaben und Funktionen, die im Zusammenhang mit der Verarbeitung personenbezogener

³ Vgl. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (GDPR); Gesetzesvertretendes Dekret Nr. 196 vom 30. Juni 2003, angepasst an die Bestimmungen der Verordnung (EU) 2016/679 durch das Gesetzesvertretende Dekret Nr. 101 vom 10. August 2018; Gesetzesvertretendes Dekret Nr. 51/2018 betreffend die „Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“; Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union und zum freien Datenverkehr“.

Daten stehen, eigens hierfür benannten natürlichen Personen übertragen werden, die unter ihrer Aufsicht arbeiten.⁴

In diesem Zusammenhang sind für die Bearbeitung von Meldungen, Offenlegungen oder Anzeigen Personen zu benennen, die von den für die Datenverarbeitung Verantwortlichen ausdrücklich ermächtigt und zuvor zu diesem Zweck geschult worden sind.⁵

Dabei sollte der interne organisatorische Aufbau jeder Stelle berücksichtigt werden, sodass die Ermächtigungen zur Datenverarbeitung alle Personen betreffen, die an der Bearbeitung von Meldungen beteiligt sind (z. B. für den Fall, dass die Meldung irrtümlich über Protokolle und nicht über die richtigen Kanäle eingeht).

Diese Personen müssen außerdem eine angemessene und spezifische berufliche Ausbildung erhalten, um ihre fachlichen Fähigkeiten auch im Hinblick auf die Rechtsvorschriften zum Schutz personenbezogener Daten, zur Daten- und Informationssicherheit sowie in Bezug auf Schulungen zu den eingerichteten Verfahren zu stärken.

Gemäß den Bestimmungen über den Schutz personenbezogener Daten und des gesetzvertretenden Dekrets Nr. 24/2023 müssen die für die Datenverarbeitung Verantwortlichen, die Auftragsverarbeiter und die für die Verarbeitung personenbezogener Daten befugten Personen sich insbesondere an die folgenden Grundsätze halten:

- Sie müssen die Daten auf eine rechtmäßige, korrekte und gegenüber den betroffenen Personen transparente Weise verarbeiten („Rechtmäßigkeit, Korrektheit und Transparenz“).
- Sie müssen die Daten ausschließlich zum Zweck der Bearbeitung von Meldungen und zum Zweck von Offenlegungen oder Anzeigen seitens der durch das Gesetzesvertretende Dekret Nr. 24/2023 geschützten Personen sammeln („Einschränkung der Zielsetzung“).
- Sie müssen sicherstellen, dass nur jene Daten, die für die Erreichung der Zielsetzungen relevant und unbedingt erforderlich sind, genutzt oder verarbeitet werden („Datenminimierung“). In diesem Zusammenhang legt das Dekret fest, dass personenbezogene Daten, die nicht offensichtlich für die Bearbeitung einer bestimmten Meldung erforderlich sind, nicht erhoben werden oder, falls sie versehentlich erhoben werden, unverzüglich gelöscht werden.
- Sie müssen gewährleisten, dass die Daten korrekt sind und, falls notwendig, auf den neuesten Stand gebracht werden; es sind alle angemessenen Maßnahmen zu ergreifen, damit ungenaue Daten, die sich auf eine konkrete Meldung, Offenlegung oder Anzeige beziehen, rechtzeitig gelöscht oder berichtigt werden („Genauigkeit“).
- Sie müssen die Daten in einer Form aufbewahren, die die Identifizierung der betroffenen Personen ermöglicht, und zwar für den Zeitraum, der für die Bearbeitung der spezifischen Meldung erforderlich ist, in jedem Fall aber nicht länger als fünf Jahre ab dem Datum der Mitteilung über das endgültige Ergebnis des Meldeverfahrens (siehe Artikel 14 des Gesetzesvertretenden Dekrets Nr. 24/2023) („Einschränkung der Datenaufbewahrung“).
- Sie müssen die Daten durch geeignete technische und organisatorische Maßnahmen

⁴ Vgl. Art. 2-quaterdecies des gesetzvertretenden Dekrets Nr. 196/2003 in geltender Fassung.

⁵ Vgl. Artikel 29 und 32, Absatz 4, der Verordnung (UE) 2016/679.

verarbeiten, sodass eine angemessene Sicherheit der personenbezogenen Daten gewährleistet ist, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor versehentlichem Verlust sowie versehentlicher Zerstörung oder Beschädigung („Integrität und Vertraulichkeit“). Im vorliegenden Kontext, der zahlreiche Risiken für die Rechte und Freiheiten der betroffenen Personen aufweist, ist in der Regel der Einsatz von Verschlüsselungstools im Rahmen der internen Kanäle und des externen Meldekanals als geeignete Maßnahme zu betrachten, um den oben genannten Grundsatz der Integrität und Vertraulichkeit – angefangen mit dem Entwurf des Kanals und durch datenschutzfreundliche Voreinstellungen – umzusetzen. Die getroffenen Sicherheitsmaßnahmen müssen in jedem Fall regelmäßig überprüft und aktualisiert werden.

- Sie müssen ein Modell für die Bearbeitung der Meldungen in Übereinstimmung mit den Grundsätzen des Schutzes personenbezogener Daten festlegen; es sind insbesondere technische und organisatorische Maßnahmen ab dem Entwurf des Meldekanals (Privacy by Design) zu ergreifen; zudem muss sichergestellt werden, dass durch datenschutzfreundliche Voreinstellungen (Privacy by Default) nur jene personenbezogenen Daten verarbeitet werden, die für die entsprechende Meldung, öffentliche Bekanntgabe oder Anzeige unbedingt erforderlich sind. Insbesondere müssen diese Maßnahmen sicherstellen, dass personenbezogene Daten ohne das Eingreifen des Verantwortlichen oder einer befugten Person nicht automatisch einer unbestimmten Anzahl von Personen zugänglich gemacht werden.
- Sie müssen eine Datenschutz-Folgenabschätzung in der Entwurfsphase des Meldekanals und somit vor Beginn der Datenverarbeitung durchführen, um die Risiken für alle beteiligten Personen (Whistleblower, gemeldete Personen, Dritte) zu bewerten und geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein Sicherheitsniveau zu gewährleisten, das der Eintrittswahrscheinlichkeit und Schwere der ermittelten Risiken angemessen ist (siehe Artikel 13).
- Sie müssen den potenziell betroffenen Personen (z. B. Hinweisgeber, gemeldete Personen, von der Meldung betroffene Personen, Mittler usw.) eine Datenschutzbelehrung mittels Veröffentlichung von Unterlagen zum Datenschutz übermitteln, z. B. über eine Website oder eine Plattform und durch die Übermittlung kurzer Informationen zum Datenschutz anlässlich der Nutzung anderer vom Dekret vorgesehenen Kanäle. Gemäß Artikel 13 und 14 der EU-Verordnung 2016/679 müssen diese Informationen zum Zeitpunkt der Erhebung der personenbezogenen Daten bereitgestellt werden und eine Reihe spezifischer Angaben enthalten. Diese Informationen können beispielsweise in den von der Einrichtung/Körperschaft für die Bearbeitung von Meldungen erlassenen organisatorischen Leitfaden aufgenommen oder in einem gesonderten Abschnitt, der für die Erfassung und Bearbeitung von Meldungen verwendeten IT-Anwendung veröffentlicht werden. Hierbei handelt es sich etwa um die Identität und die Kontaktdaten des für die Datenverarbeitung Verantwortlichen, des Auftragsverarbeiters, sofern vorhanden, und der zur Datenverarbeitung berechtigten Person, den Zweck der Verarbeitung von personenbezogenen Daten sowie um die Rechtsgrundlage der Verarbeitung und die Dauer der Speicherung personenbezogener Daten. Es sollten jedoch keine Ad-hoc-Informationen an die verschiedenen betroffenen Personen geliefert werden (auch um einen allzu großen Informationsfluss zu vermeiden, aus dem die Beteiligung der entsprechenden Person an einer Meldung abgeleitet werden kann, wodurch die Schutzmaßnahmen zur Vertraulichkeit zunichte gemacht werden). Die für die Datenverarbeitung Verantwortlichen, die Auftragsverarbeiter und die zur Verarbeitung personenbezogener Daten befugten Personen

müssen zudem:

- das Verzeichnis der Verarbeitungstätigkeiten, das mit Informationen im Zusammenhang mit der Erfassung und Verwaltung von Meldungen zu ergänzen ist, aktualisieren;
- das Verbot der Rückverfolgbarkeit von Meldekanälen gewährleisten; erfolgt der Zugriff auf die internen Kanäle und auf den externen Meldekanal über das interne Datennetzwerk des Verpflichteten mittels Firewall oder Proxies, muss die Nicht-Rückverfolgbarkeit des Hinweisgebers – sowohl auf der IT-Plattform als auch auf den gegebenenfalls an der Übertragung oder Überwachung der Kommunikation beteiligten Netzwerkgeräten – zum Zeitpunkt der Herstellung der Verbindung zu diesen Kanälen gewährleistet sein;
- sofern möglich, die Rückverfolgbarkeit der durch das befugte Personal durchgeführten Aktivitäten unter Einhaltung der Sicherheitsvorkehrungen zum Schutz des Hinweisgebers zu gewährleisten, um den Missbrauch von Daten im Zusammenhang mit der Meldung zu vermeiden. Die Rückverfolgbarkeit von Informationen, die Rückschlüsse auf die Identität oder die Tätigkeit des Hinweisgebers erlauben, muss vermieden werden.

Darüber hinaus kann die Aufbewahrung der Meldungen und der dazugehörigen Unterlagen für den Zeitraum, der für deren Feststellung erforderlich ist, in jedem Fall aber nicht länger als fünf Jahre ab dem Datum der Mitteilung des endgültigen Ergebnisses des Meldeverfahrens, unter Einhaltung der Schutzmaßnahmen zur Vertraulichkeit und des in der DSGVO festgelegten Grundsatzes der Einschränkung der Datenaufbewahrung verlängert werden.

Schließlich müssen die Körperschaften ihre Beziehungen zu etwaigen Dienstleistern, die in ihrem Namen personenbezogene Daten verarbeiten (wie zum Beispiel Anbieter der IT-Plattform, die als Kanal für den Empfang und die Verwaltung von Meldungen verwendet wird, sofern Letztere mit der Systemverwaltung beauftragt sind), mit einem Datenverarbeitungsvertrag, d. h. mit einem Abkommen zur Verarbeitung personenbezogener Daten gemäß Art. 28 der DSGVO (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“) oder gemäß Art. 18 des Gesetzesvertretenden Dekrets Nr. 51/2018 zur „Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Prävention, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“ regeln.

1.2.7 Schutz vor Repressalien

Der Schutz vor Repressalien stützt sich im Wesentlichen auf den Schutz vor jeder Form von Vergeltung, auch wenn diese nur versucht oder angedroht wird. In diesem Zusammenhang hat der nationale Gesetzgeber einen weit gefassten Begriff der Repressalie akzeptiert, der gemäß Artikel 2 Absatz 1 Buchstabe m) wie folgt beschrieben wird: „Jedes Verhalten, jede Handlung oder Unterlassung, auch wenn diese nur versucht oder angedroht wird, die aufgrund der Meldung, der Anzeige an die Gerichts- oder Rechnungsprüfungsbehörden oder Offenlegung erfolgt und die dem Hinweisgeber oder der Person, die die Anzeige erstattet hat, direkt oder indirekt einen ungerechtfertigten Schaden zufügt oder zufügen kann“.

Im Artikel 17 Absatz 4 des Gesetzesvertretenden Dekrets Nr. 24/2023 werden mögliche

Vergeltungsmaßnahmen beschrieben, allerdings ohne Anspruch auf Vollständigkeit, etwa Kündigung, eine nicht erfolgte Beförderung, Disziplinarmaßnahmen, eine nicht erfolgte Verlängerung oder eine vorzeitige Beendigung eines befristeten Arbeitsvertrags, Schädigungen anderer Art, u. a. auch Reputationsschäden „insbesondere durch die sozialen Medien“, negative Bewertungen, Aufgabenwechsel, Änderung der Arbeitszeit. Nach Ansicht der ANAC kann als Repressalie auch Folgendes gelten: die Forderung von Ergebnissen, die auf die angegebene Art und Weise und im vorgegebenen Zeitraum nicht erzielt werden können; eine willkürlich erteilte negative Leistungsbeurteilung; ein ungerechtfertigter Widerruf von Aufträgen; eine ungerechtfertigte Nichterteilung von Aufträgen bei Zuweisung derselben an eine andere Person; die wiederholte Ablehnung von Anträgen (z. B. Urlaub, Wartestände).⁶

Im Falle des Hinweisgebers obliegt es demjenigen, der das Verhalten, die Unterlassungen oder die Handlungen vorgenommen hat, nachzuweisen, dass dieses Verhalten auf Gründe zurückzuführen ist, die nichts mit der Meldung zu tun haben.

Schließlich hat die Missachtung des Verbots zweierlei Folgen:

- die Nichtigkeit der Handlungen, die unter Missachtung des Verbots vorgenommen wurden;
- die Verhängung einer Geldbuße zwischen 10.000 und 50.000 Euro durch die ANAC.

1.2.8 Haftungsbeschränkungen

Haftungsbeschränkungen stellen einen zusätzlichen Schutz dar (siehe Art. 20): Der Hinweisgeber ist im Hinblick auf die Offenlegung und Verbreitung bestimmter Kategorien von Informationen weder strafrechtlich noch zivilrechtlich oder verwaltungsrechtlich strafbar.⁷

Dieser Schutz gilt sofern folgende zwei Aspekte gewährleistet sind:

- der Whistleblower hat zum Zeitpunkt der Meldung hinreichende Gründe für die Annahme, dass alle offengelegten Informationen für die Aufdeckung des Verstoßes erforderlich sind;
- die Meldung ist in Übereinstimmung mit den gesetzlichen Bestimmungen erfolgt.

⁶ vgl. erläuternder Bericht zu den Leitlinien zum Schutz von Personen, die Verstöße gegen das Unionsrecht und nationale Rechtsvorschriften melden, genehmigt durch ANAC-Beschluss Nr. 311 vom 12. Juli 2023;

⁷ vgl. erläuternder Bericht des Gesetzesvertretenden Dekrets Nr. 24/2023: Die Verletzung des Amts- und Berufsgeheimnisses, die Verletzung der Bestimmungen zum Schutz des Urheberrechts oder des Schutzes personenbezogener Daten und die mögliche Verletzung des Rufs der betroffenen Person aufgrund der Meldung oder Verbreitung von Informationen sind nicht strafbar bzw. ahndbar.

II. Analyse des Ist-Zustands

2.1 Whistleblowing in der Landesverwaltung

Mit ihrem Beschluss Nr. 1113/2023 betreffend „Whistleblowing-Verfahren für die Bearbeitung von Meldungen von Informationen über Verstöße“ hat die Landesregierung, nach Anhörung der Gewerkschaften, die bisherigen Verfahren für die Bearbeitung von Meldungen an die neuen Bestimmungen der Richtlinie (EU) 2019/1937 und des Gesetzesvertretenden Dekrets Nr. 24/2023 angepasst, indem sie unter den verschiedenen Meldekanälen eine eigene IT-Plattform vorgesehen und das Verfahren neu geregelt hat.

In Bezug auf das Whistleblowing, auf die Meldeverfahren und Meldekanäle wurden über den entsprechenden Abschnitt der institutionellen Webseite ([provinz.bz.it/de/home](https://recht.provinz.bz.it/de/home)) - <https://recht.provinz.bz.it/de/whistleblower>) Informationen über Verstöße veröffentlicht.

Um das Landespersonal zu sensibilisieren und zu informieren, wurde zudem eine Mitteilung über myNET zum Thema Genehmigung des neuen Whistleblowing-Verfahrens veröffentlicht; darüber hinaus wurden eine kurze Erläuterung der Ziele des Whistleblowings und Informationen zur neuen IT-Plattform veröffentlicht, versehen mit einem Link zum Abschnitt der institutionellen Webseite, der dem betreffenden Thema gewidmet ist und von dem aus auf die Plattform zugegriffen werden kann (<https://recht.provinz.bz.it/de/whistleblower>).

Derzeit enthält der Verhaltenskodex des Personals in der geltenden Fassung weder Vorschriften noch Verweise zu Bestimmungen zum Whistleblowing. Nach Angaben der Mitglieder der Arbeitsgruppe wird der Kodex aktualisiert und es wird erwartet, dass in der neuen Fassung ein Artikel zu diesem Thema eingefügt wird.

2.1.1 IT-Plattform

Bei der IT-Plattform handelt es sich um die Plattform „Südtirol | Home (integrityline.com)“, die von der EQS Group im Auftrag der SIAG AG erstellt wurde.

Die Plattform sieht eine geführte Eingabe der Meldedaten vor, informiert zum bzw. verwaltet den Datenschutz und bietet Tools für die Bearbeitung der Unterlagen im Rahmen der Überprüfung.

Die Bearbeitung der Meldungen erfolgt direkt und ausschließlich durch internes Personal der Landesverwaltung.

In jedem Fall können die Meldungen anonymisiert werden, sodass die Daten zur Identität des Hinweisgebers und der betroffenen Personen für jene, die sich normalerweise der Meldung annehmen, nicht automatisch einsehbar bzw. nur in begründeten Fällen einsehbar sind. Auch die Gespräche nach der Meldung erfolgen anonym.

Wenn aus Überprüfungsgründen andere Personen als die Bearbeiter der Meldung über den Inhalt der Meldung und/oder die beigefügten Unterlagen informiert werden müssen, werden die personenbezogenen Daten geschwärzt. Der Zugriff auf die gesamte Meldung ist nämlich auf die

Mitglieder der eigens dafür eingesetzten Arbeitsgruppe beschränkt. Die anderen Personen, die nach und nach eventuell in die Überprüfung einbezogen werden können, haben keinen Zugang zu den Daten zur Identität des Hinweisgebers.

Für jede Meldung und für jede Aktivität wird ein Überarbeitungsprotokoll erstellt, dank dem direkt vom System aus in das gesamte Überarbeitungsverfahren und in das Editing Einsicht genommen werden kann. Die Aktivitäten der Systemnutzer sind unter Einhaltung der Sicherheitsvorkehrungen zum Schutz des Hinweisgebers nachverfolgbar.

Schließlich bietet die Plattform eine Vielzahl an interaktiven Dashboards und Grafiken (mit Daten wie der durchschnittlichen Anzahl der Tage, die für den Abschluss von Meldungen erforderlich sind, der Anzahl der laufenden Fälle, der Anzahl der Fälle nach Typologien, der Fallanalyse nach geografischem Raum, Sitz oder Abteilung) sowie Suchfunktionen für die Datenanalyse und die anschließende Berichterstattung. Alle Informationen können im Excel-Format heruntergeladen werden.

Die Anbieter des IT-Systems haben spezifische Garantien in Bezug auf die Sicherheitsmaßnahmen vorgesehen; die Plattform sieht nämlich Verschlüsselungstools vor, um die Vertraulichkeit der Daten während der Übertragung und im Ruhezustand sowie den Schutz vor Cyberangriffen zu gewährleisten. Die in den Meldungen enthaltenen personenbezogenen Daten und die im Zuge der Überprüfungen erhobenen Daten werden in einer „besonders sicheren“ Datenbank des Anbieters gespeichert. Der dazugehörige Server befindet sich innerhalb der Europäischen Union und alle in der Datenbank gespeicherten Daten sind verschlüsselt. Im Rahmen des Abschlusses des Liefervertrags der Anwendung wurde der Lieferant zum externen Auftragsverarbeiter ernannt.

In diesem Zusammenhang wurden bereits vor der Umsetzung zwei getrennte Stellungnahmen des DPO (Data Protection Officer) eingeholt, die beide zur Umsetzung der SIAG übermittelt wurden, auch in Bezug auf die technischen Sicherheitsmaßnahmen.

Nach der Implementierung wurde die Folgenabschätzung (Data Protection Impact Assessment, DPIA) – die darauf abzielt, die Datenschutzrisiken für alle an der Verarbeitung der betreffenden Daten beteiligten Personen zu analysieren und geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Sicherheitsniveau zu gewährleisten – am 18.03.2024 aktualisiert, anschließend vom Datenschutzbeauftragten positiv bewertet⁸ und in das KRC-System (Knowledge Risk Compliance) hochgeladen.⁹

⁸ Der Datenschutzbeauftragte hat in seiner Stellungnahme einige Empfehlungen für die Durchführung der Verarbeitung in Übereinstimmung mit den geltenden Rechtsvorschriften zum Schutz und zur Wahrung personenbezogener Daten abgegeben. Der Datenschutzbeauftragte hat empfohlen, bei der Abwicklung aller Datenströme und -verarbeitungsverfahren für personenbezogene Daten auch in Zukunft auf die in der Verordnung (EU) 2016/679 vorgesehenen Grundsätze zu achten. Er hat insbesondere folgende Hinweise gegeben:

„Es wird darauf hingewiesen, dass der für die Datenverarbeitung Verantwortliche in jedem Fall verpflichtet ist, die Grundsätze des Datenschutzes zu beachten, darunter die Grundsätze der „Rechtmäßigkeit, der Korrektheit und der Transparenz“, der „Einschränkung der Zielsetzung“, der „Datenminimierung“ und der „Einschränkung der Datenspeicherung“, nach denen die personenbezogenen Daten „in rechtmäßiger, korrekter und transparenter Weise gegenüber der betroffenen Person verarbeitet werden müssen“, „zu bestimmten, ausdrücklichen und rechtmäßigen Zwecken erhoben und anschließend so verarbeitet werden müssen, dass sie mit diesen Zwecken nicht unvereinbar sind“, „angemessen, relevant und auf das für die Zwecke, für die sie verarbeitet werden, erforderliche Maß beschränkt sind“ und „in einer Form aufbewahrt werden müssen, die die Identifizierung der betroffenen Personen für einen Zeitraum ermöglicht, der

2.1.2 Weitere Meldekanäle

Um das Meldesystem für alle potenziellen Nutzer zugänglich zu machen, können schriftliche Meldungen in Papierform händisch abgegeben oder über den Postdienst verschickt werden. Die Meldung muss in diesen Fällen in einem versiegelten Umschlag mit der Aufschrift „persönlich-privat“ abgegeben werden.

Um die Meldung zu verfassen, kann der Hinweisgeber das hierfür vorgesehene und auf der institutionellen Webseite der Landesverwaltung veröffentlichte Formular (<https://diritto.provincia.bz.it/it/whistleblower>) ausfüllen.

Möchte der Hinweisgeber das von der Verwaltung zur Verfügung gestellte Formular nicht verwenden, so kann seine Meldung von der Verwaltung dennoch entgegengenommen werden, sofern diese hinreichend detailliert ist und die Meldung keinen Ausschlussfall darstellt¹⁰.

die Erreichung der Zwecke, für die sie verarbeitet werden, nicht überschreitet“. (Artikel 5 Absatz 1 Buchstaben a), b), c) und e) der Verordnung).

- *Es wird empfohlen, die Verarbeitung zu überwachen, um im Laufe der Zeit alle Änderungen oder Ergänzungen, die hinsichtlich der Rechtsvorschriften über den Schutz und die Verarbeitung personenbezogener Daten relevant sein könnten, zu überprüfen.*
- *Es wird zudem empfohlen, regelmäßige Audits beim Anbieter der Whistleblowing-Meldeplattform vorzusehen, um die Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen im Laufe der Zeit zu überwachen.*
- *Es wird empfohlen, die Genehmigungsschreiben für die Datenverarbeitung gegenüber Personen innerhalb der Einrichtung des für die Datenverarbeitung Verantwortlichen regelmäßig zu erstellen und zu unterzeichnen. Es wird weiters empfohlen, den zur Verarbeitung befugten Personen angemessene Anweisungen zu erteilen und entsprechende Schulungen anzubieten;*
- *Um das Risiko für die Rechte und Freiheiten der betroffenen Personen zu minimieren, wird empfohlen, das Bewusstsein der für die Verarbeitung Verantwortlichen ständig zu stärken und die Informationen über die Datenverarbeitung und die Dokumentation zur Verarbeitung, einschließlich der vorliegenden Folgenabschätzung, zu ergänzen, falls dies angesichts künftiger Änderungen der Verarbeitung personenbezogener Daten erforderlich ist, um die Dokumentation und die durchgeführte Analyse auf dem neuesten Stand zu halten.*
- *Es wird weiters empfohlen, keine zusätzlichen und übermäßigen Datenverarbeitungen durchzuführen, die sich von den unbedingt erforderlichen unterscheiden und darüber hinausgehen – diese Datenverarbeitungen sind rechtswidrig und entbehren jeder Rechtsgrundlage;*
- *Es wird auch darauf hingewiesen, wie wichtig es ist, auf eine punktuelle Bearbeitung möglicher Verstöße gegen den Schutz personenbezogener Daten („Datenverluste“) zu achten, die sich auf die verarbeiteten personenbezogenen Daten in Bezug auf die vorgesehenen gesetzlichen Obliegenheiten beziehen;*
- *Der DPO empfiehlt dem Verantwortlichen, auf Neuerungen und Problematiken gemäß den Grundsätzen des privacy by design und des privacy by default aufmerksam zu machen.*

⁹ KRC ist das Anwendungsportale des Landes für die Führung und Aktualisierung des Registers der Datenverarbeitung im Sinne von Art. 30 der VO (EU) 2016/679.

¹⁰ Laut dem von der Landesregierung vorgesehenen Verfahren werden folgende Punkte im Rahmen der Überprüfung nicht berücksichtigt, außer es liegt ein Antrag auf Ergänzung vor:

- *Meldungen zu Vorkommnissen, die weder mit dem Personal noch mit einem Leistungsbereich der Landesverwaltung zu tun haben;*
- *anonym eingereichte Meldungen;*
- *Meldungen, die ausschließlich auf Verdachtsmomente oder Gerüchte Bezug nehmen, sowie Meldungen, die allgemein bekannte Tatsachen beschreiben;*

Meldungen in Papierform müssen in jedem Fall vom Hinweisgeber unterschrieben werden; weiters ist eine Ausweiskopie beizulegen. Um die Privatsphäre des Hinweisgebers zu schützen, wird empfohlen, die Meldung von der Ausweiskopie zu trennen, indem die Kopie des Ausweises in einen zweiten, kleineren, geschlossenen Umschlag gesteckt wird. Der kleine Umschlag muss, zusammen mit der Meldung, in den größeren Umschlag gesteckt werden, der dann bei der angegebenen Adresse abgegeben oder dieser per Post zugestellt werden muss.

Alternativ kann über die entsprechende IT-Plattform eine Sprachnachricht aufgezeichnet werden; die Software ändert die Stimme des Hinweisgebers automatisch ab, sodass diese nicht mehr erkennbar ist; die dazugehörige Audiodatei wird dann von der Software abgespeichert.

Es ist auch möglich, ein Treffen mit dem Verantwortlichen für Korruptionsvorbeugung und Transparenz zu beantragen. Während des Treffens kann der Hinweisgeber Erklärungen zur Meldung abgeben, von denen ein Protokoll erstellt werden wird. Der Hinweisgeber ist dazu berechtigt, das Protokoll einzusehen, Änderungen desselben zu beantragen und es durch seine Unterschrift zu bestätigen.

Gemäß dem von der Landesregierung mit genanntem Beschluss angewandten Verfahren stellt das Einreichen einer Meldung in anonymisierter Form einen Ausschlussfall dar. Die Landesverwaltung kann jedoch auch bei in anonymisierter Form eingelangten Meldungen angemessene und erforderliche Kontrollen durchführen, sofern die Meldung detailliert genug ist.

2.1.3 Die für die Verwaltung der Meldungen verantwortliche Person

Im obgenannten Beschluss der Landesregierung wird der Verantwortliche für Korruptionsvorbeugung und Transparenz (RPCT) als die Person bezeichnet, an welche die Meldungen zu richten sind und die für deren Verwaltung verantwortlich ist; der RPCT verfügt über eine kleine Arbeitsgruppe, die sich aus dem Direktor des Amtes für institutionelle Angelegenheiten und einem hierfür bevollmächtigten Mitarbeiter zusammensetzt; sollte eines der Mitglieder der Arbeitsgruppe abwesend oder verhindert sein, kann der RPCT einen „anderen Bediensteten seines Amtes“ mit der Durchführung der Überprüfung beauftragen.

In der Folge wurden die jeweiligen Personen ernannt: Die ernannten Personen sind berechtigt, personenbezogene Daten zu verarbeiten, es ist ihnen untersagt, überschüssige Daten zu erheben und sie sind verpflichtet, versehentlich erfasste Daten sofort zu löschen.

Für diese Personen wurde ein erster Weiterbildungslehrgang ausgerichtet, und derzeit werden weitere Fortbildungen angeboten.

De facto wurden die eingelangten Meldungen vom RPCT bearbeitet; die Mitglieder der Arbeitsgruppe

- Beanstandungen, Forderungen oder Anträge im Zusammenhang mit einem persönlichen Interesse des Hinweisgebers, die ausschließlich mit seinem persönlichen Arbeits- oder öffentlichem Anstellungsverhältnis oder dem eigenen Arbeitsverhältnis mit hierarchisch übergeordnetem Personal zusammenhängen;

- Meldungen von Verstößen, die bereits durch die Europäische Union oder durch nationale Rechtsakte, welche in Teil II des Anhangs zum Gesetzesvertretenden Dekret Nr. 24 vom 10. März 2023 angeführt sind, oder durch nationale Rechtsakte verbindlich geregelt sind, welche die Akten der Europäischen Union laut Teil II des Anhangs zur EU-Richtlinie 2019/1937 umsetzen, auch wenn diese nicht in Teil II des Anhangs zum Gesetzesvertretenden Dekret Nr. 24, vom 10. März 2023 angeführt sind.“

haben bisher operative und unterstützende Tätigkeiten ausgeübt.

2.1.4 Das Verfahren zur Verwaltung der Meldungen

In Bezug auf das Verfahren zur Verwaltung der Meldungen gemäß den Bestimmungen des Gesetzesdekrets Nr. 24/2023 wird vorgesehen, dass der Erhalt binnen 7 Tagen bestätigt wird. Dem Hinweisgeber ist es über eine IT-Plattform stets möglich, den Bearbeitungsstand seiner Meldung einzusehen; weiters kann er durch die Eingabe eines persönlichen Zugangscode auf einen verschlüsselten Informationskanal zugreifen, um mit der Körperschaft ins Gespräch zu treten.

In jedem Fall wird der Hinweisgeber während der Verwaltung der Meldung stets auf dem Laufenden gehalten; innerhalb von drei Monaten erhält er Feedback zu den durchgeführten Maßnahmen, und nach Abschluss der Untersuchung wird ihm das Endergebnis mitgeteilt.

Gemäß den Erklärungen der obgenannten Mitglieder der Arbeitsgruppe sind die detaillierten Ergebnisse der Meldungen in internen Vermerken vertraulicher Natur festgehalten.

Der Verantwortliche für Korruptionsvorbeugung und Transparenz schließt das Verfahren innerhalb von drei Monaten nach Erhalt der Meldung ab und nimmt einen der folgenden Schritte vor:

- Je nach Zuständigkeit erfolgt eine Übermittlung der Meldung an die Gerichtsbehörde, den Rechnungshof und/oder die ANAC, sofern die Meldung zur Gänze oder teilweise stichhaltig ist.
- Es werden die für Disziplinarverfahren zuständige Stelle und/oder andere zuständige Organisationseinheiten über den gemeldeten Vorfall unterrichtet, damit geeignete Maßnahmen ergriffen werden können.
- Die Meldung wird archiviert, sollte die Überprüfung ergeben, dass diese haltlos ist.

Im Verfahren ist nicht ausdrücklich vorgesehen, dass die Ergebnisse der Untersuchung der Meldung für die Korruptionsvorbeugung verwendet werden können.

Halbjährlich ergreift der Verantwortliche für Korruptionsvorbeugung und Transparenz auch formelle Archivierungsmaßnahmen: Somit werden Meldungen, denen nicht weiter nachgegangen werden kann, und für die keine Überprüfung eingeleitet wird, gemeinsam archiviert¹¹. In jenen Maßnahmen, die im Abschnitt Transparente Verwaltung auf der Webseite des Landes veröffentlicht werden, werden die Meldungen und die Ergebnisse ihrer Überprüfung in jedem Fall in aller Kürze beschrieben, um weder Rückschlüsse auf den Verfasser der Meldung noch auf deren Inhalt zuzulassen.

Innerhalb von 5 Jahren nach Abschluss des Falls werden die Daten und Unterlagen gelöscht.

In diesem Zusammenhang ist es möglich, sich über die IT-Plattform sogenannte „Reminder“ schicken zu lassen, um dann ein Feedback zu geben und die Meldungen händisch zu löschen.

2.1.5. Eingelangte Meldungen

In den letzten drei Jahren war die Gesamtzahl der Meldungen überschaubar (9 Meldungen insgesamt), davon sind zwei Meldungen in anonymisierter Form erfolgt.

¹¹ Es handelt sich um die in der vorhergehenden Fußnote genannten Ausschlussfälle.

In Bezug auf die Nutzung der Meldekanäle ist anzumerken, dass die Hinweisgeber das auf der Webseite des Landes veröffentlichte Meldeformular nur sehr wenig genutzt haben; die Meldungen sind über die herkömmlichen Meldekanäle eingetroffen, über den Postdienst oder indem eine Mail an das eigens hierfür eingerichtete E-Mail-Postfach whistleblower@provinz.bz.it gesendet wurde.

Bei den Hinweisgebern handelte es sich um Bedienstete, selbstständige Mitarbeiter, anonyme Hinweisgeber oder Bürger.

Wie in den verschiedenen in den letzten Jahren genehmigten Dreijahresplänen für Korruptionsvorbeugung und Integrierten Tätigkeits- und Organisationsplänen (PIAOs) beschrieben, haben die bis dato eingereichten Meldungen nach Einschätzung der Mitglieder der Arbeitsgruppe im Bereich der Korruptionsvorbeugung keine besonderen Probleme aufgeworfen.

2.2 „Whistleblowing“ in der Agentur für Energie Südtirol – KlimaHaus

Die Agentur für Energie Südtirol - KlimaHaus (im Folgenden „Agentur“) hat in Übereinstimmung mit den europäischen und nationalen Rechtsvorschriften ein Verfahren für die Entgegennahme und Verwaltung von Meldungen implementiert.

In Bezug auf das Whistleblowing, die Modalitäten und Kanäle für Meldungen wurde über einen speziellen Abschnitt der institutionellen Website <https://www.klimahaus.it/de/willkommen-bei-uns-1.html> kommuniziert. Das dort einsehbare FAQ-Dokument „*Whistleblowing*“ enthält Informationen zur Verwaltung des Whistleblowings durch die Agentur, zu meldepflichtigen Verstößen, zur Person, welche die Meldung entgegennimmt, zu den Meldekanälen, den Maßnahmen zum Schutz des Hinweisgebers und zum Schutz der Vertraulichkeit der Identität des Hinweisgebers.

Die Meldungen werden im Organisations-, Verwaltungs- und Kontrollmodell (MOGC) gemäß gesetzesvertretendem Dekret Nr. 231/2001 angeführt; darüber hinaus wurden die Verwaltungsverfahren im Dokument „Beschluss des Generaldirektors Nr. 2024/33 vom 19.7.2024, Aktualisierung der Whistleblowing-Richtlinien“ im Detail festgelegt.

Schließlich wurde mit Beschluss des Generaldirektors Nr. 2024/59 vom 2.12.2024 der Ethikkodex überarbeitet, der auf den Anhang 1 „Whistleblowing-Richtlinien und FAQ“ als integrierenden Bestandteil verweist.

Es sei hinzugefügt, dass im Ethikkodex bei Verstößen gegen den vertraulichen Umgang mit den Identitäten des Hinweisgebers und anderer beteiligter Personen ausdrücklich verschiedene Arten disziplinarischer Verantwortung vorgesehen sind.

2.2.1 Die IT-Plattform

Die Agentur hat einen internen Telekommunikationskanal eingerichtet. Die Meldungen auf elektronischem Wege erfolgen über die Website – Transparente Körperschaft – Whistleblowing der Agentur für Energie Südtirol – KlimaHaus, oder über die Online-Plattform SAFETIPS, die eigens für die Verwaltung des Whistleblowing entwickelt wurde.

Die Plattform bietet eine Anleitung zur Eingabe der Meldung, stellt Datenschutzerklärungen bereit, verwaltet diese und bietet Werkzeuge zur Verwaltung des Überprüfungsablaufs an.

Der Meldekanal ermöglicht es den Hinweisgebern, anonym Meldungen vorzunehmen und ohne ihre Identität preiszugeben mit dem Whistleblowing-Beauftragten zu kommunizieren.

Um ein angemessenes Schutzniveau zu gewährleisten, hat die Software-Firma INOOVA bei der Implementierung der SAFETIPS-Plattform technische und organisatorische Maßnahmen ergriffen, die im Dokument „Technisch-organisatorische Maßnahmen“ (TOM) beschrieben sind.

Die Meldungen werden anonymisiert, damit die Angaben zur Identität des Hinweisgebers und der beteiligten Personen nur in begründeten Fällen von der Person, welche die Meldung verwaltet, eingesehen werden können. Der Whistleblowing-Beauftragte erhält die Meldung in verschlüsselter Form; auch weitere Gespräche nach Erhalt der Meldung erfolgen anonym.

Die Informationseingabe und die gesamte Bearbeitung der Kommunikation erfolgt auf den Servern der INOOVA GmbH. Die Server befinden sich in Deutschland in einem nach DIN ISO/IEC 27001-Norm zertifizierten Rechenzentrum.

Im Rahmen des Abschlusses des Dienstleistungsvertrags für das Anwendungsmanagement wurde gemäß Artikel 28 der DSGVO (EU-Verordnung EU 2016/679) mit der INOOVA GmbH eine Vereinbarung über die Verarbeitung personenbezogener Daten erstellt und unterzeichnet.

Das gesamte Meldeverfahren, die Daten und Dokumente, die auf der Plattform hochgeladen werden, werden ohne Cookies und ohne IP-Adressen-Tracking oder -Logging automatisch in Form eines SSL-Protokolls (Secure Sockets Layer) verschlüsselt¹². Anschließend werden die Daten vom Browser über das verschlüsselte Protokoll an den Server übertragen.

Die Datenbank ist verschlüsselt, und der Zugriff auf ihren Inhalt ist, nach vorheriger Eingabe von Benutzernamen und Passwort, nur autorisierten Personen möglich.

Es wurde eine Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) durchgeführt, um die Gefahren für die Privatsphäre aller an der Verarbeitung der jeweiligen Daten Beteiligten zu analysieren und geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Sicherheitsniveau zu gewährleisten; diese DPIA wurde vom Datenschutzbeauftragten (DSB) am 07.02.2024 positiv bewertet.

2.2.2 Andere Meldekanäle

Neben den Meldungen über die obgenannte IT-Plattform können die Meldungen auch per E-Mail an das Aufsichtsgremium des Organisations-, Verwaltungs- und Kontrollmodells (MOGC), odv@agenziacasaclima.it, geschickt werden.

¹² SSL-Protokolle sind Standardprotokolle zum Schutz der Kommunikation im Internet. Sie stellen sicher, dass sensible Daten, die von Nutzern im Internet bereitgestellt werden, vertraulich behandelt werden und in keiner Weise von Dritten abgefangen werden; dies erfolgt dank verschlüsselter Kommunikation zwischen dem Client-Server und dem Webserver.

Eine mündliche Meldung ist alternativ dazu nicht vorgesehen.

2.2.3 Für die Verwaltung der Meldungen und die dazugehörigen Verfahren zuständige Personen

Die Verwaltung der Meldungen über die IT-Plattform erfolgt direkt und ausschließlich durch den Verantwortlichen für Korruptionsvorbeugung und Transparenz (RPCT) der Agentur, welcher zur Verarbeitung der entsprechenden Daten befugt ist.

Es wurde mitgeteilt, dass diese zuständige Person zu den Bestimmungen in den Bereichen Datenschutz, Datensicherheit und Management der gesamten Datenverwaltungsverfahren angemessen geschult wurde.

Neben dem Verantwortlichen für Korruptionsvorbeugung und Transparenz hat der IKT-Verantwortliche in seiner ausschließlichen Funktion als Systemadministrator Zugriff auf die Online-Plattform.

Wie auf der Informationsseite der Website beschrieben, umfasst das Verwaltungsverfahren im Einklang mit den europäischen und nationalen Rechtsvorschriften verschiedene Phasen. Es wird jedoch nicht ausdrücklich auf die Verpflichtung hingewiesen, innerhalb von sieben Tagen eine Empfangsbestätigung der Meldung zu übermitteln.

In den letzten drei Jahren sind keine Meldungen eingegangen.

2.3 Whistleblowing im Institut für den sozialen Wohnbau (WOBI)

Das Institut für den sozialen Wohnbau der Autonomen Provinz Bozen, in der Folge als „WOBI“ bezeichnet, hat folgende Meldekanäle vorgesehen:

- Meldung per E-Mail an die E-Mail-Adresse: whistleblower@pec.wobi.bz.it;
- Sendung über den Postdienst. In diesem Fall sollte die Meldung in einem versiegelten Umschlag mit der Aufschrift „persönlich-vertraulich“, an den Verantwortlichen für Korruptionsvorbeugung adressiert werden; der Meldung ist eine Ausweiskopie beizufügen, die unterschrieben werden muss. Um die Vertraulichkeit des Absenders zu gewährleisten, wird empfohlen, die Meldung von der Kopie des Ausweisdokuments zu trennen und die Kopie des Dokuments in einen zweiten, kleineren, geschlossenen Umschlag zu stecken. Der kleine Umschlag wird in den größeren Umschlag gesteckt, der per Post versandt wird;
- eine mündliche Meldung, einschließlich einer Erklärung, die in Anwesenheit des Verantwortlichen für Korruptionsvorbeugung abgegeben wird; die Erklärung wird verschriftlicht.

Auf der Webseite des WOBI, wird unter *Menü > Transparente Verwaltung > Weitere Inhalte > Vorbeugung der Korruption* darüber informiert, dass für die Abgabe schriftlicher Meldungen ein Meldeformular erstellt wurde; dieses ist jedoch nicht auf derselben Seite abrufbar.

Die Meldung kann auch in vollständig anonymisierter Form erfolgen, sofern eine ausreichende Begründung vorliegt.

In den letzten drei Jahren sind keine Meldungen eingegangen.

III. Schlussfolgerungen

Auf der Grundlage der erhaltenen Informationen und durchgeführten Überprüfungen, werden, im Hinblick auf eine mögliche Verbesserung, einige Anregungen und Empfehlungen gegeben, für die in einem Jahr ein Follow-up stattfinden soll.

3.1 Die Südtiroler Landesverwaltung

Die Südtiroler Landesverwaltung hat die Meldeverfahren an die neuen Bestimmungen der Richtlinie (EU) 2019/1937 und des Gesetzesvertretenden Dekrets Nr. 24/2023 angepasst. Als weiterer Meldekanal wurde etwa eine IT-Plattform eingerichtet und das Verfahren neu geregelt. Auch die Organisation und das Verfahren scheinen angemessen.

In Bezug auf die Maßnahmen zum Schutz der Vertraulichkeit der Identität des Hinweisgebers wird vorgeschlagen, eine Person mit der Verwahrung der Identität des Hinweisgebers zu beauftragen; in den ANAC-Leitlinien ist eine solche Person fakultativ und nicht obligatorisch vorgesehen; diese dient als mögliche zusätzliche Garantie für den Schutz der Vertraulichkeit der Identität des Hinweisgebers.

Bei derjenigen Person, die mit dem Schutz der Vertraulichkeit der Identität des Hinweisgebers beauftragt ist, handelt es sich im Wesentlichen um einen Dritten. Dieser ist befugt, der für die Entgegennahme der Meldung verantwortlichen Person, auf deren ausdrücklichen und begründeten Antrag hin, Zugriff zur Identität des Hinweisgebers zu gewähren. Die Identität des Hinweisgebers ist dem Verwahrer der Identität nicht bekannt; dieser verarbeitet die Daten des Hinweisgebers und die in der Meldung enthaltenen Daten nicht direkt, sondern erteilt, sofern erforderlich, nur eine Genehmigung.

Sollte der Verantwortliche für Korruptionsvorbeugung und Transparenz der Landesverwaltung, da die Mitglieder der entsprechenden Arbeitsgruppe abwesend oder verhindert sind, die Überprüfung einem anderen Bediensteten seines Amtes anvertrauen, so ist darauf hinzuweisen, dass auch für diese Person die organisatorischen Maßnahmen sowie die Sicherheitsmaßnahmen Anwendung finden müssen, die für die Mitglieder der Arbeitsgruppe vorgesehen sind (z. B. eine Genehmigung zur Verarbeitung personenbezogener Daten, eine diesbezügliche Fortbildung usw.).

In Bezug auf die abschließende Phase der Überprüfung und etwaige alternative Maßnahmen ist die mögliche Berücksichtigung der Ergebnisse der Meldung zum Zwecke der Verhinderung des Korruptionsrisikos und der entsprechenden Aktualisierung des PIAO nicht ausdrücklich vorgesehen. Es wird empfohlen, das Verfahren auch angesichts der möglichen Tragweite der Meldungen und ihrer Auswirkungen auf die Risikobewertung entsprechend zu ergänzen.

In Bezug auf den Verhaltenskodex des Personals der Autonomen Provinz Bozen wird darauf hingewiesen, dass seine geltende Fassung die Vorschriften zum Whistleblowing nicht enthält und/oder auch nicht auf diese verweist, sondern im Gegenteil vorsieht, dass Unregelmäßigkeiten an den Vorgesetzten gemeldet werden.¹³

Laut Angaben der Mitglieder der Arbeitsgruppe wird der Verhaltenskodex derzeit überarbeitet und es wird erwartet, dass in der neuen Fassung ein Artikel zu diesem Thema eingefügt wird.

In diesem Zusammenhang wird empfohlen, die Aktualisierungsphase innerhalb eines hierfür angemessenen Zeitraums abzuschließen, indem der Artikel 5 neu formuliert wird und auf die wichtigsten Elemente des Whistleblowings sowie auf das von der Verwaltung vorgesehene Melde- und Verwaltungsverfahren verwiesen wird. Um den Verhaltenskodex an den aktuellen Rechtsrahmen anzupassen, muss auch eine disziplinarrechtliche Verantwortlichkeit, der für die Bearbeitung der Meldungen zuständigen Personen vorgesehen werden, falls die Verpflichtung zum Schutz des vertraulichen Umgangs mit der Identität des Hinweisgebers und anderer Personen, deren Identität geschützt werden muss, verletzt wird.

3.2 Agentur für Energie Südtirol – KlimaHaus

Die Agentur hat die Meldeverfahren an die neuen Bestimmungen der Richtlinie (EU) 2019/1937 und des Gesetzesvertretenden Dekrets Nr. 24/2023 angepasst; in diesem Rahmen wurde auch eine IT-Plattform als Meldekanal eingerichtet und das von den Gesetzesbestimmungen vorgesehene Verfahren übernommen.

Abgesehen davon, was der Landesverwaltung in Bezug auf die mit dem Verwahren der Identität beauftragte Person vorgeschlagen wurde, wird darauf hingewiesen, dass keine alternativen Formen mündlicher Meldungen vorgesehen sind, was im Gesetzesvertretenden Dekret Nr. 24/2023 hingegen ausdrücklich vorgesehen ist. Um allen die Möglichkeit zu geben, Meldungen einzureichen, sollte das Verfahren ergänzt und auch diese Form der Meldung ermöglicht werden, wie von den nationalen Rechtsvorschriften bereits vorgesehen.

¹³ Artikel 5 Absatz 5 des Verhaltenskodex lautet wie folgt:

„4. Wir halten uns an die Vorschriften des geltenden Antikorruptionsplans und arbeiten mit dem oder der Antikorruptionsbeauftragten zusammen, wenn immer dies erforderlich ist. Erhalten wir Kenntnis von einem rechtswidrigen Verhalten innerhalb der Verwaltung, melden wir dies dem/der Vorgesetzten; aufrecht bleibt dabei die Pflicht, strafrechtlich relevante Sachverhalte der Gerichtsbehörde zu melden.“

3.3 Das Institut für den sozialen Wohnbau (WOBI) der Autonomen Provinz Bozen

Das Institut hat die Meldeverfahren noch nicht an die neuen Bestimmungen der EU-Richtlinie 2019/1937 und des Gesetzesvertretenden Dekrets Nr. 24/2023 angepasst; in diesem Zusammenhang hat das WOBI erklärt, "*damit begonnen zu haben, die Verfahren zum Ankauf einer IT-Plattform einzuleiten*".

In diesem Sinne wird eine rasche Anpassung empfohlen, wobei insbesondere die IT-Plattform eingerichtet werden sollte, über die Meldungen vor allem auf digitalem Wege eingereicht werden können, und eine angemessene Information im Internet vorzusehen ist.

Der auf der Webseite des WOBI unter *Menü > Transparente Verwaltung > weitere Inhalte > Vorbeugung der Korruption* erwähnte Vordruck zur Meldung unerlaubter Handlungen, der derzeit auf derselben Webseite nicht abrufbar ist, sollte auf der Webseite des Instituts zur Verfügung gestellt werden.

16.12.2024

Gez.
Cinzia Flaim

Gez.
Irmgard Prader



Prüfstelle
39100 Bozen | Freiheitsstraße 66
Organismo di valutazione
39100 Bolzano | Corso Libertà, 66

Tel. 0471 402 212 | Fax 0471 260 114
pruefstelle@landtag-bz.org | organismovalutazione@consiglio-bz.org
PEC: pruefstelle.organismovalutazione@pec.prov-bz.org
www.landtag-bz.org/de/pruefstelle.asp
www.consiglio-bz.org/it/organismo-di-valutazione.asp