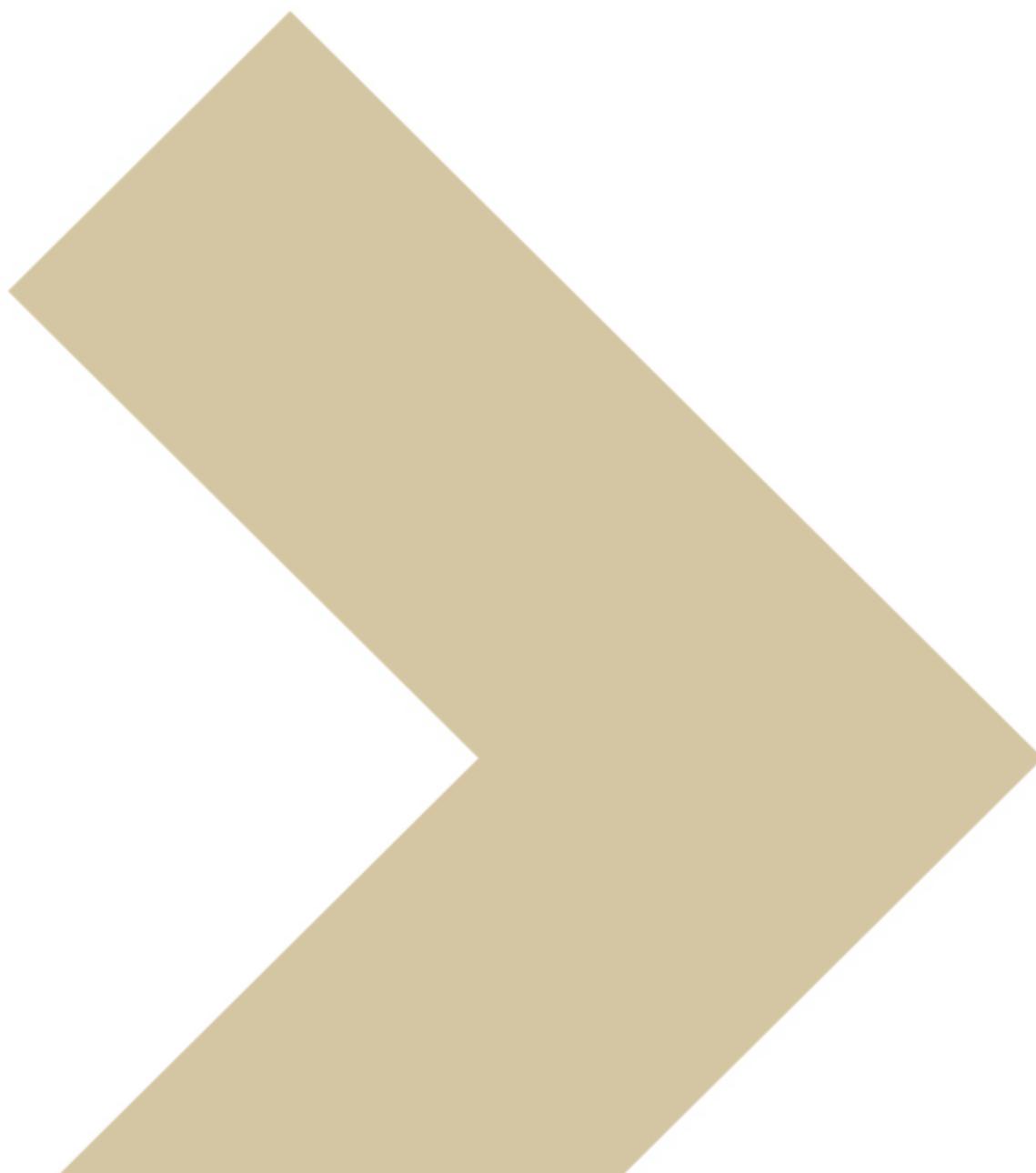




## Leistungsbeschreibung 2023



## Abkürzungsverzeichnis und Glossar

BITMi	Bundesverband <u>IT-Mittelstand</u>
CEO	CEO steht für "Chief Executive Officer" und ist die US-amerikanische Bezeichnung für den Geschäftsführer einer Firma oder einer Organisation
FedRAMP	Das Federal Risk and Authorization Management Program ist ein regierungsweites Programm der USA, das einen standardisierten Ansatz für die Sicherheitsbewertung, Autorisierung und kontinuierliche Überwachung von Cloud-Produkten und -Diensten bietet.
HinSchG	Hinweisgeberschutzgesetz
HIPAA	Health Insurance Portability and Accountability Act Ein US-Gesetz zum Geheimhaltungsstandard
LkSG	Lieferkettensorgfaltspflichtengesetz
Open Web Application Security Project (OWASP)	Das Open Web Application Security Project ist eine Non-Profit-Organisation mit dem Ziel, die Sicherheit von Anwendungen und Diensten im World Wide Web zu verbessern.
Pentesting/Penster	Beauftragung eines IT-Unternehmens mit dem Ziel, Schwachstellen in den Sicherheitsvorkehrungen einer Software zu entdecken. Ziel ist es, mögliche Schlupflöcher für unerlaubte Zugriffe / Hackerangriffe auf die Software aufzudecken und entsprechende Gegenmaßnahmen zu ergreifen.
RegTech	RegTech ist ein Kofferwort aus dem englischen Begriff „Regulatory Technology“. Wie bei Fintech geht es um den Einsatz von innovativer Technologie. Der Fokus liegt bei RegTech allerdings auf der von innovativen Technologien gestützten effektiveren und effizienteren Abbildung, Erfüllung und Dokumentation regulatorischer und aufsichtlicher Pflichten. Auch wenn RegTech vor diesem Hintergrund für eine Vielzahl an Wirtschaftsbereichen relevant sein könnte, soll für diesen Beitrag unter RegTech allein „RegTech für den Finanzsektor verstanden werden.

	<p>Eine allgemeingültige Definition von RegTech gibt es nicht. Die Begriffsbestimmungen von Institutionen wie dem Finanzstabilitätsrat FSB, der Europäischen Bankenaufsichtsbehörde EBA und der Bank für Internationalen Zahlungsausgleich BIZ haben jedoch gemeinsam, dass sie RegTech als Anwendung innovativer Finanztechnologie durch beaufsichtigte Institute zur Erfüllung regulatorischer Anforderungen definieren. Aufgrund der Unterstützung von Compliance- Anforderungen findet sich in der Literatur für RegTech zuweilen auch der Begriff Comptech.</p>
SaaS	Software as a Service
SOC	Ein Security Operations Center ist ein Zentrum, das Dienstleistungen für die IT-Sicherheit bietet: ein Verfahren zur Vorbeugung und Behandlung von unvorhergesehenen Schwierigkeiten.
SOC 1	Ein Bericht nach Service Organization Control 1 oder SOC 1 (ausgesprochen "Sock One") ist eine schriftliche Dokumentation interner Kontrollmechanismen. SOC 1 wird in Typ 1- und Typ 2-Berichte unterteilt. Typ 1 berichtet darüber, wie angemessen die Kontrollmechanismen einer Service-Organisation zu einem bestimmten Zeitpunkt bzw. Datum sind, während Typ 2 eine Aussage zur Wirksamkeit der Kontrollmechanismen über einen längeren Zeitraum trifft. SOC 1-Berichte werden von einem Service-Auditor erstellt.
Trustworthy Computing Security Development Lifecycle	Trustworthy Computing Security Development Lifecycle ist ein 2004 von Microsoft veröffentlichtes Konzept zur Entwicklung von sicherer Software, die böswilligen Angriffen standhalten muss.

## „Implementierung eines Meldesystems“

### 1 Unternehmensangaben

#### 1.1 Name und Adresse des Bieters

Firmenname	dsgvoNORD GmbH
Straße / Postfach	Marga-Faulstich-Str. 8
PLZ und Ort	24145 Kiel
Telefon / Telefax	0431-301400600
E-Mail / Internet	info@dsgvo-nord.de
Ansprechpartner	Manuel Langeheinecke, CEO

#### 1.2 Rechtsform

hinweis.de ist eine Marke und Leistung der dsgvoNORD GmbH.

### 2 Technische Leistungsfähigkeit

#### 2.1 Einfacher Zugang per Link auf der Unternehmenswebseite für Interne und Externe mit jedem digitalen Endgerät und browserunabhängig.

Unsere App ist auf allen internetfähigen Eingabegeräten, bis hin zum Smartphone nutzbar.

#### 2.2 Einbindungsfähigkeit in Homepage

Die Einbindung Ihres Meldekanals erfolgt einfach mittels Platzierung des Links und/oder des QR-Codes. Es ist keine Einbindung in Ihre IT nötig.

#### 2.3 Verfügbarkeit 24/7- 365 Tage

Unsere App ist rund um die Uhr verfügbar. Wir sichern eine 99,8%ige Erreichbarkeit zu.

#### 2.4 Gewährleistung der Vertraulichkeit der Daten – Datenschutz konforme Bearbeitung personenbezogener Daten (DSGVO); kein möglicher Zugriff durch Dritte

Ihre Daten sind bei uns sicher! Höchste Sicherheit für Ihre Daten ist für uns selbstverständlich und eine unerlässliche Voraussetzung für erfolgreiche Whistleblowing-Lösungen. hinweis.de ist DSGVO-konform und wird bei der

Hetzner GmbH gehostet. Informationen zu den Meldungen können ausschließlich von den Systemberechtigten des Unternehmens oder dafür vom Unternehmen bestellten Dienstleister (z.B. Ombudsmann) gesehen und bearbeitet werden. Meldende Personen können über eine individuelle PIN die Daten zu ihrer Meldung und die Antworten des Unternehmens sehen. Darüber hinaus hat niemand Zugang zu den Informationen.

Der Zugriff auf das Meldestellenportal kann ausschließlich über eine 2-Faktor-Authentifizierung erfolgen, was wir ausdrücklich empfehlen.

## **2.5 Darstellung und Berücksichtigung von rechtlichen länderspezifischen Besonderheiten**

Sobald veränderte nationale Gesetze zur Umsetzung der EU-Hinweisgeber-Richtlinie verabschiedet werden, werden wir entsprechende nationale Versionen zur Verfügung stellen und fortlaufend an die jeweilig vorherrschenden, gesetzlichen Anforderungen anpassen.

## **2.6 Daten Hosting in Deutschland**

Das hinweis.de Meldesystem ist bei der Hetzner GmbH gehostet und hat dadurch das Sicherheitsniveau erster Klasse. Die dsGvoNORD GmbH und sämtliche Dienstleister haben Ihren Sitz aussch. in Deutschland und damit innerhalb der EU. Die Daten sind in Rechenzentren in Deutschland gehostet.

## **2.7 Aufbewahrung bzw. Archivierung der eingegangenen Meldungen**

Die Anforderungen zur Datenarchivierung und -löschung sind DSGVO-konform umgesetzt. Die gesetzliche vorgegebene Aufbewahrungspflicht ist im System hinterlegt. Die fristgemäße Löschung erfolgt automatisch, Bearbeitende werden zuvor mehrfach an die nahende Frist erinnert.

## **2.8 Flexibilität für meldende Personen: Anonyme oder offene Meldung und Möglichkeit mit Bearbeitern vertraulich zu kommunizieren**

Die Anonymität des Hinweisgebers und die Anforderungen zur Datenlöschung sind DSGVO-konform umgesetzt und zu jeder Zeit sichergestellt. Alle sensiblen Daten sowie Chatnachrichten sind in der Anwendung verschlüsselt und werden bei der Hetzner GmbH gehostet; auch deren Verschlüsselungstechnik entspricht dem Stand der Technik. Sollte sich die meldende Person für eine offene Meldung entscheiden, wird im System deutlich darauf hingewiesen, dass die Anonymität verloren geht. Auf diese Weise wird sichergestellt, dass die meldende Person keine persönlichen Daten preisgibt, wenn sie dies nicht ausdrücklich wünscht. Entscheidet sich die meldende Person hingegen für eine anonyme Meldung, bleibt diese wie bisher anonym.

Der Zugriff auf personenbezogene Daten der meldenden Person ist auf eine spezielle Rolle beschränkt, um die Vertraulichkeit der Daten zu gewährleisten. Nur berechtigte Benutzer haben Zugriff auf diese Informationen, um die Privatsphäre der meldenden Person zu schützen. Zudem können Benutzer, die

Zugriff auf diese Daten haben, den Zugriff auf die persönlichen Informationen bearbeiten und für andere Benutzer die Einsicht in diese Daten autorisieren.

## **2.9 Möglichkeit die Meldung in unterschiedlichen Sprachen abzugeben**

hinweis.de bietet neben Deutsch und Englisch 10 weitere zusätzlich buchbare Sprachen an: Französisch (fra), Italienisch (ita), Niederländisch (nld), Polnisch (pol), Portugiesisch (por), Rumänisch (ron), Russisch (rus), Spanisch (spa), Tschechisch (ces), Ungarisch (hun).

## **2.10 Einfache Installation mit der Möglichkeit der Nutzung von Standardvorlagen und Standardfragestellungen hinsichtlich Bereichseinordnung**

Das System ist von allen Anwendenden intuitiv bedienbar und barrierefrei. Meldungen können über einen strukturierten Fragebogen in Textform und auch telefonisch abgegeben werden. Sollten Meldende die Bereichseinordnung unzutreffend vorgenommen haben, können die Bearbeiter dies dem zutreffenden Bereich zuordnen. Dazu können sind auch Standardantworten an den Meldenden im System hinterlegt, die vom Unternehmen angepasst werden können.

## **2.11 Flexibilität bei der Berechtigungsvergabe**

Unser Meldesystem bietet ein abgestuftes Berechtigungskonzept, das von der Einsicht in alle Meldungen bis zum Lesen einzeln freigegebenen Fällen reicht. Es besteht die Möglichkeit, mit dem Meldenden über einen Chat in unmittelbaren Austausch zu treten.

## **2.12 Hosting von Impressum- und Datenschutzinformationen sowie Anzeige in der App**

Unsere Kunden können Ihr Impressum und Ihre Datenschutzerklärung in unserer Anwendung hochladen und mit den Seiten im Meldeportal verlinken. Wir bieten hierfür eine Hosting-Funktion an. Sie können Ihre Dokumente auch in verschiedenen Sprachen hochladen.

## **2.13 Möglichkeit einer Erinnerungsfunktion für die Benachrichtigung nach Meldungseingang sowie nach 3 Monaten der Fallbearbeitung**

Gemäß den Vorgaben der EU-Richtlinie muss spätestens vor Ablauf von 7 Kalendertagen eine Eingangsbestätigung über den Empfang der Meldung versendet werden. Dies erfolgt über die integrierte Chatfunktion. Der oder die Verantwortliche(n) der Meldestelle werden über eingehende Meldungen informiert und an die Versendung der Eingangsbestätigung bzw. die Mitteilung über Folgemaßnahmen per E-Mail erinnert.

Hinweise können bei längerer Inaktivität eskalieren. Stellvertreter der zugeordneten Bearbeiter erhalten automatisch Zugriff sowie eine Benachrichtigung per E-Mail. Der Zeitraum vor Fristablauf ist frei konfigurierbar.

## 2.14 Dashboard mit Kennzahlen für ein entsprechendes Compliance-Reporting

Über das „Dashboard“ können Analysen zu Berichtskategorien, Bearbeitungszeiten und anderen Themen erstellt werden. Dies kann auch heruntergeladen werden.

Falls noch zwischen Organisationseinheiten oder Standorten unterschieden werden soll, könnten die Standorte als „Tochterunternehmen“ angelegt werden, um für diese eine separate Bearbeitung und Auswertung zu ermöglichen. Dieses können wir auch nach Ihren Bedürfnissen noch ergänzen.

## 2.15 Erfahrung und Begleitung der Implementierung in mitbestimmungspflichtigen Unternehmen (auch vor Ort)

Viele Unternehmen des deutschen Mittelstands vertrauen bereits hinweis.de als Meldesystem. Wie schon bei einer Vielzahl von Kunden umgesetzt, unterstützen wir auch Sie mit unserer Expertise im Dialog mit den entsprechenden Interessenvertretern (bspw. dem Betriebsrat, Geschäftsleitung etc.).

## 2.16 Erweiterung des Systems für Zwecke der Berichterstattung für durchgeführte interne Untersuchungen durch Unternehmen oder dessen Dienstleister

Als SaaS-Lösung sind Individualisierungen der Software grundsätzlich nicht vorgesehen. Sofern dies im Einzelfall gewünscht wird, wird ein nach Aufwand berechneter Stundensatz vereinbart. Ergebnisse der internen Untersuchungen können und sollten im Vorgang auf der hinweis.de Plattform abgelegt werden.

## 2.17 IT-Sicherheitskonzept (Cyber Security, Zertifizierungen) des Dienstleisters sowie der IT-Infrastruktur

Die Server der Hetzner GmbH – auf dem das Meldesystem gehostet wird – sind u.a. ISO 27001 zertifiziert.

Neben der ISO27001 zertifiziertem Rechenzentrum, welches eine hohe IT-Sicherheit gewährleistet, wird das Hinweisgebersystem regelmäßig von der [Breaking-Labs GmbH](#) nach internationalen Standards (OWASPv4) untersucht.

Etwaige Schwachstellen werden regelmäßig mittels sogenannter Penetrationstests ermittelt und geschlossen.

### 3 Beschreibung der Lösung im Detail

#### 3.1 Unser Meldesystem

hinweis.de bietet für mündliche und schriftliche Meldungen eine passende Lösung für mittelständische Unternehmen zwischen 50 und 15.000 Mitarbeitern; und dies alles ohne IT-Implementierung über eine Cloud-Lösung.

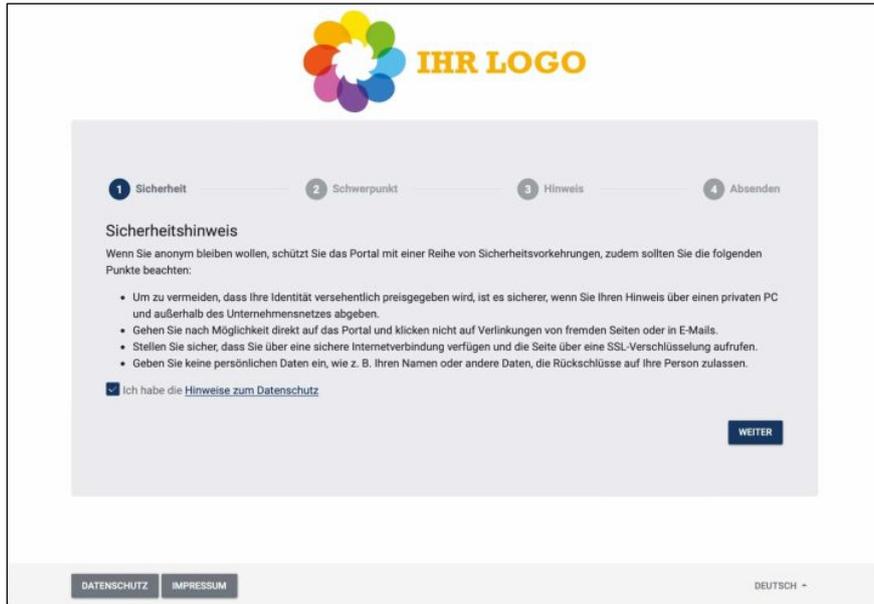
Unser Meldesystem ist unmittelbar nach der Buchung zugänglich und nutzbar; sie funktioniert unabhängig von der IT des Unternehmens (Plug & Play-Lösung). Meldende Personen können somit Meldungen mit jedem internetfähigen Gerät abgeben und die berechtigten Personen im Unternehmen können auf eingehende Meldungen ihrerseits über das Internet zugreifen, ohne im IT-System des Unternehmens eingeloggt zu sein.

The screenshot shows a web interface for reporting a violation. At the top center is a logo consisting of a colorful flower-like shape with the text 'IHR LOGO' to its right. Below the logo, the main heading is 'Verstoß melden'. Underneath, there are three paragraphs of text: the first explains the reporting process, the second states that all violations can be reported, and the third promises protection for whistleblowers. At the bottom left of this section is a dark blue button labeled 'MELDUNG ABGEBEN' and a language selector 'DEUTSCH'. To the right of the main text is a light gray box titled 'Anmelden' with a login form containing fields for 'Kennung\*' and 'Passwort\*', and an 'ANMELDEN' button. At the bottom of the page, there are links for 'DATENSCHUTZ' and 'IMPRESSUM' on the left, and a language selector 'DEUTSCH' on the right.

Interface für meldende Personen zur Eingabe von Meldungen (links) und anonyme Einsichtnahme von gegebenen Meldungen (rechts)

Meldungen, die über das Meldesystem eingereicht werden, können sowohl anonym als auch offen erfolgen. Unser System bietet dem Systemberechtigten, wie zum Beispiel den Meldestellenbeauftragten, zusätzlich zur anonymen oder offenen Meldung die Möglichkeit, über einen Chat direkt mit der meldenden Person in Kontakt zu treten. Die meldende Person kann dabei anonym bleiben.

Zu Beginn wird die Person über Sicherheits- und Datenschutzhinweise informiert und muss diese bestätigen.



The screenshot shows a web interface for a reporting system. At the top, there is a logo consisting of a colorful flower-like shape and the text "IHR LOGO". Below the logo is a progress bar with four steps: 1. Sicherheit, 2. Schwerpunkt, 3. Hinweis, and 4. Absenden. The current step is "Sicherheitshinweis". The text reads: "Wenn Sie anonym bleiben wollen, schützt Sie das Portal mit einer Reihe von Sicherheitsvorkehrungen, zudem sollten Sie die folgenden Punkte beachten:". There are three bullet points: "Um zu vermeiden, dass Ihre Identität versehentlich preisgegeben wird, ist es sicherer, wenn Sie Ihren Hinweis über einen privaten PC und außerhalb des Unternehmensnetzes abgeben.", "Gehen Sie nach Möglichkeit direkt auf das Portal und klicken nicht auf Verlinkungen von fremden Seiten oder in E-Mails.", and "Stellen Sie sicher, dass Sie über eine sichere Internetverbindung verfügen und die Seite über eine SSL-Verschlüsselung aufrufen." Below the bullet points is a checkbox with the text "Ich habe die [Hinweise zum Datenschutz](#)". A "WEITER" button is located at the bottom right of the main content area. At the bottom of the page, there are links for "DATENSCHUTZ" and "IMPRESSUM" on the left, and a language selector "DEUTSCH" with a dropdown arrow on the right.

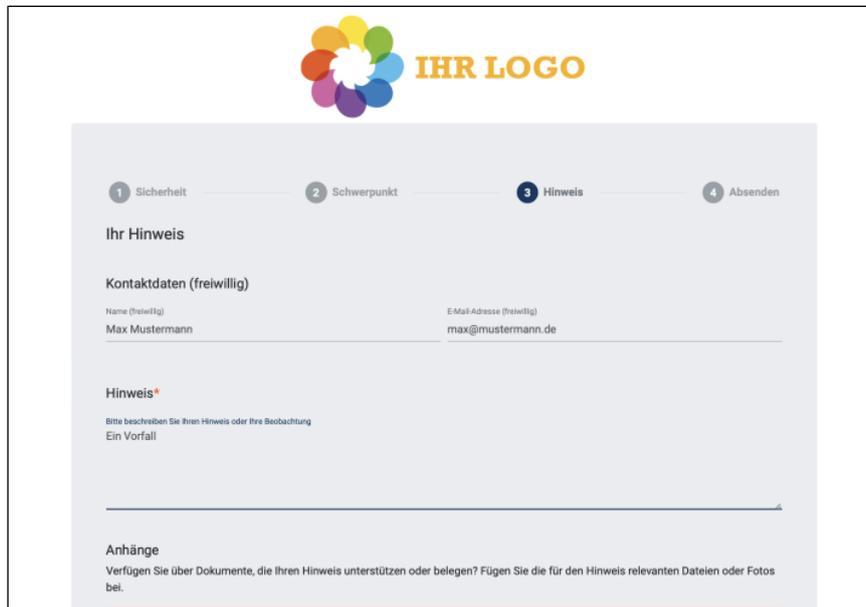
Sicherheits- und Datenschutzhinweise für die meldende Person

Meldungen werden über einen Fragebogen eingegeben. Am Ende des Fragebogens hat die meldende Person die Möglichkeit, unterstützende Dateien hochzuladen.

Schwerpunkt der Meldung auswählen (optional und frei definierbar)

Uploadbereich für Dateianhänge und Angabe weiterer Informationen

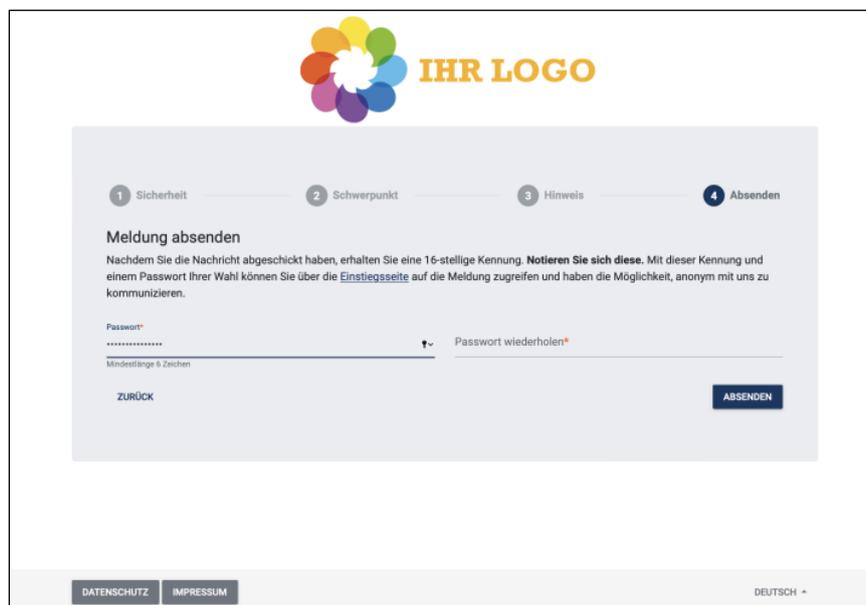
Kontaktdaten können freiwillig preisgegeben werden oder es kann anonym weiter fortgefahren werden.



The screenshot shows a web form titled "Ihr Hinweis" (Your Report) under the "IHR LOGO" header. The form is divided into four steps: 1. Sicherheit, 2. Schwerpunkt, 3. Hinweis (active), and 4. Absenden. The "Hinweis" section includes a "Kontakt Daten (freiwillig)" (optional contact data) field with "Name (freiwillig)" (Max Mustermann) and "E-Mail-Adresse (freiwillig)" (max@mustermann.de). Below this is a "Hinweis\*" (Report\*) field with the instruction "Bitte beschreiben Sie Ihren Hinweis oder Ihre Beobachtung" (Please describe your report or observation) and the example "Ein Vorfall" (An incident). At the bottom, there is an "Anhänge" (Attachments) section with the instruction "Verfügen Sie über Dokumente, die Ihren Hinweis unterstützen oder belegen? Fügen Sie die für den Hinweis relevanten Dateien oder Fotos bei." (Do you have documents that support or prove your report? Attach the relevant files or photos for the report).

Einfügen von Kontaktdaten (auch anonym) und Hinweis-Details plus Anhänge

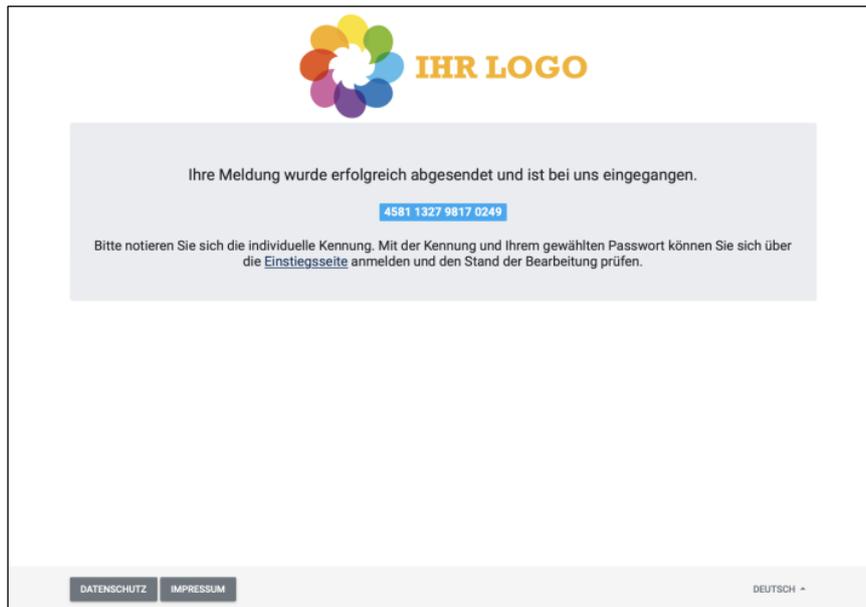
Zum Abschluss des Vorgangs muss die meldende Person ein persönliches Passwort festlegen.



The screenshot shows the "Meldung absenden" (Send Report) form. It features the same "IHR LOGO" header and step indicators (1. Sicherheit, 2. Schwerpunkt, 3. Hinweis, 4. Absenden active). The "Meldung absenden" section includes instructions: "Nachdem Sie die Nachricht abgeschickt haben, erhalten Sie eine 16-stellige Kennung. **Notieren Sie sich diese.** Mit dieser Kennung und einem Passwort Ihrer Wahl können Sie über die [Einstiegsseite](#) auf die Meldung zugreifen und haben die Möglichkeit, anonym mit uns zu kommunizieren." (After you have sent the message, you will receive a 16-digit code. **Note down this code.** With this code and a password of your choice, you can access the report via the [login page](#) and have the opportunity to communicate with us anonymously). Below the instructions are two password fields: "Passwort\*" (Password\*) and "Passwort wiederholen\*" (Repeat password\*). A note indicates "Mindestlänge 6 Zeichen" (Minimum length 6 characters). At the bottom left is a "ZURÜCK" (Back) button and at the bottom right is an "ABSENDEN" (Send) button. The footer contains "DATENSCHUTZ" (Data Protection) and "IMPRESSUM" (Imprint) links, and a language selector set to "DEUTSCH" (German).

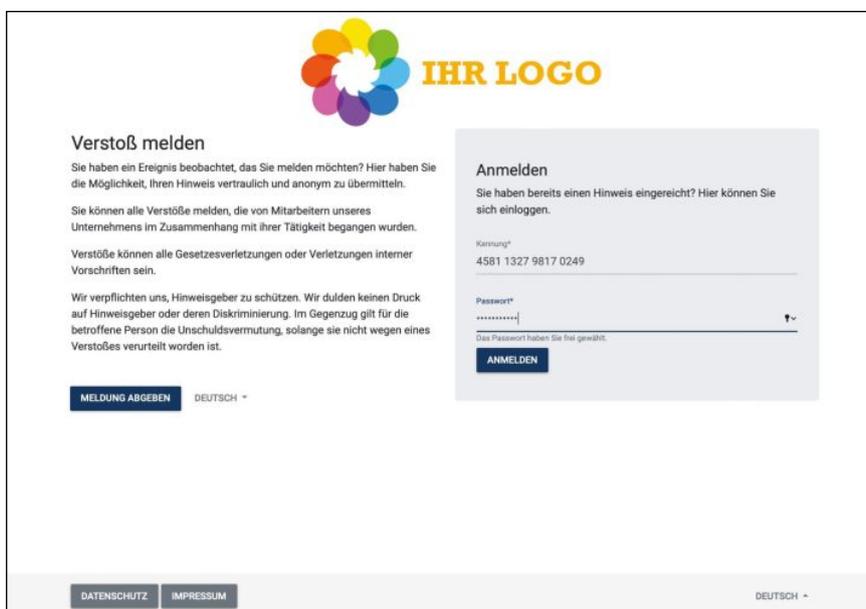
Eigenes Passwort festlegen und absenden

Im Anschluss wird eine individuelle Kennung angezeigt.



Kennung zur späteren Statusabfrage des Hinweises

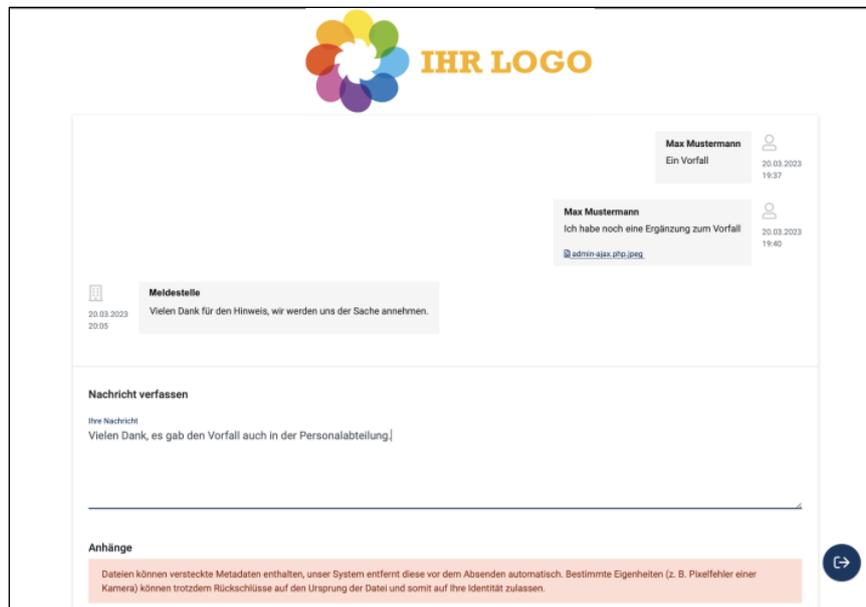
Mit diesen beiden Codes kann sich der Meldende später wieder in der betreffenden Meldung einloggen.



Login mit Kennung und Passwort

Über die Chat-Funktion können Informationen und auch weitere Dateien mit dem Unternehmen ausgetauscht werden.

Insofern die meldende Person nicht bewusst ihre Identität preisgibt, ist für den Systemberechtigten nicht ersichtlich, wer die meldende Person ist.



Kommunikationsverlauf zwischen meldender Person und den Meldestellenbeauftragten

Sollte einer der Codes (Passwort oder Zufallscode) vergessen werden, besteht für den Meldenden keine weitere Zugriffsmöglichkeit mehr. Eine Wiederherstellung der Codes ist aus Datenschutzgründen und Schutz der Anonymität des Meldenden nicht möglich. Auch seitens hinweis.de ist eine Wiederherstellung der Codes ausgeschlossen und technisch nicht möglich.

## Angenehme Nutzung für die meldende Person und Bearbeiter

Unser System besticht nicht nur durch die intuitive Führung des Meldenden bei der Berichtseingabe; auch das Meldestellenportal-Interface ist übersichtlich gestaltet.

Trotz der Einfachheit bietet das System eine Fülle an Funktionen, von denen hier nur die essenziellsten vorgestellt werden.

#	Status	Thema	Letzte Änderung
6497 9899 7710 1246	Neu	Korruption oder Bestechung	26.09.2023
2728 6899 1350 7070	Neu	Sonstiger straf- oder bußgeldbewehrter Verstoß	14.09.2023
1824 4589 1247 1025	Neu	Mobbing oder Belästigung	05.09.2023
6155 5312 9764 6988	Neu	Diebstahl, Unterschlagung oder Betrug	14.08.2023
0105 2606 3268 4180	Neu	Sonstiger straf- oder bußgeldbewehrter Verstoß	08.08.2023
2324 4159 6656 0755	Neu	Verstoß gegen Datenschutzvorschriften oder IT-Sicherheitsrichtlinien	08.08.2023
0112 2188 8758 9973	Neu	Diebstahl, Unterschlagung oder Betrug	03.08.2023
1624 3816 3512 4077	In Bearbeitung	Sonstiger straf- oder bußgeldbewehrter Verstoß	01.08.2023
7342 2716 7420 1385	Neu	Sonstiger straf- oder bußgeldbewehrter Verstoß	17.07.2023
5583 7985 9929 3770	Neu	Diebstahl, Unterschlagung oder Betrug	12.07.2023
9687 9126 6819 6962	Neu	Korruption oder Bestechung	04.07.2023
0154 0975 6665 6949	Neu	Diebstahl, Unterschlagung oder Betrug	23.06.2023
3930 7002 2925 8221	Neu	Sonstiger straf- oder bußgeldbewehrter Verstoß	23.06.2023
2167 8882 0178 5919	Neu	Verstoß gegen Umweltschutzvorschriften	19.06.2023
3894 1014 9798 8754	Neu	Mobbing oder Belästigung	16.06.2023
4139 8262 4823 6204	Neu	Diebstahl, Unterschlagung oder Betrug	25.05.2023

Übersicht und Status der eingegangenen Hinweise

## hinweis.de hilft dem Bearbeiter

Der meldenden Person muss binnen 7 Tagen der Eingang ihrer Meldung bestätigt werden. Dies erfolgt bei einem Eingang Portal automatisch vom System. Frei konfigurierbare Eskalationsstufen erinnern den Bearbeiter und Stellvertreter vor Ablauf der Rückmeldefrist.

### Eskalation

Hinweise können bei längerer Inaktivität eskalieren. Stellvertreter der zugeordneten Bearbeiter erhalten automatisch Zugriff sowie eine Benachrichtigung per E-Mail.

**Bei Status = Neu**



0 = deaktiviert

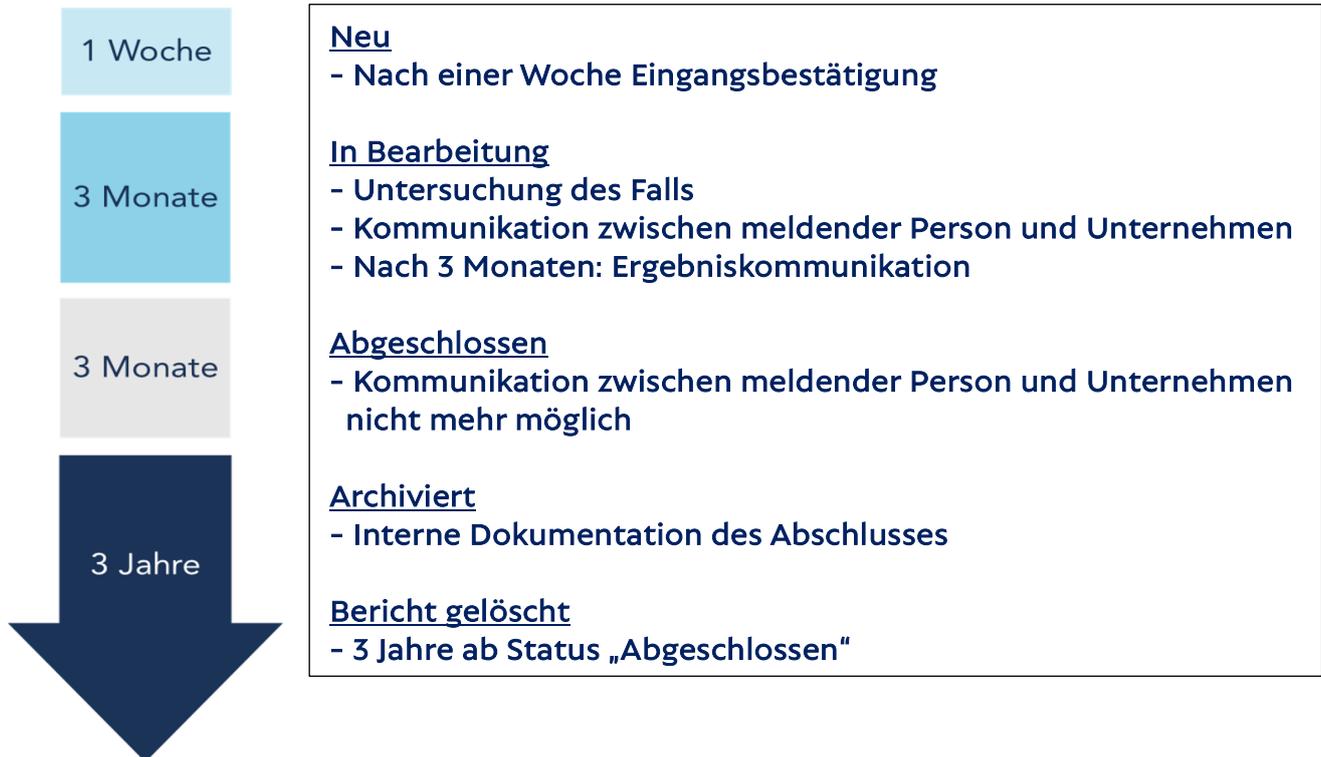
**Bei Status = In Bearbeitung**



0 = deaktiviert

Demnach informiert das System nicht nur den Bearbeiter über die zu beachtenden Fristen, sondern nimmt ihm durch Automatisierung Schritte im Prozess ab. Es unterstützt außerdem den Bearbeiter bei einer DSGVO-konformen Handhabung eines jeden Falles.

Im Folgenden eine Übersicht zu den Vorgaben der EU-Richtlinie und DSGVO, die vom Bearbeiter beachtet werden müssen und bei denen das System unterstützt:



### Systemunabhängige Dokumentation

Sowohl die meldende Person als auch der Bearbeiter haben jederzeit die Möglichkeit sich der konkreten Meldung mit allen enthaltenen Informationen auf das eigene System herunterzuladen.

Somit können die Berichte auch außerhalb unseres Systems abgespeichert werden.



### **Berechtigungskonzept**

Unser Meldesystem bietet ein abgestuftes Berechtigungskonzept, das von der Einsicht in alle Meldungen bis zu einzeln freigegebenen Fällen reicht.

#### **Administrator**

- Die Admin-Rolle ist die höchste Rolle und hat die Möglichkeit, sämtliche Organisationseinstellungen zu sehen und zu bearbeiten, Benutzer hinzuzufügen, Berechtigungen zu erteilen und Zahlungseinstellungen zu bearbeiten.
- Zusätzlich kann ein Admin auch alle Meldungen sehen und bearbeiten.
- Ein Admin kann andere Benutzer für einzelne Meldungen zum Benutzer oder Reader machen.
- Admins werden über eingehende Meldungen informiert.
- Achtung: Mindestens eine Admin-Rolle muss vergeben werden; aber auch mehrere Admins sind möglich.

### Benutzer

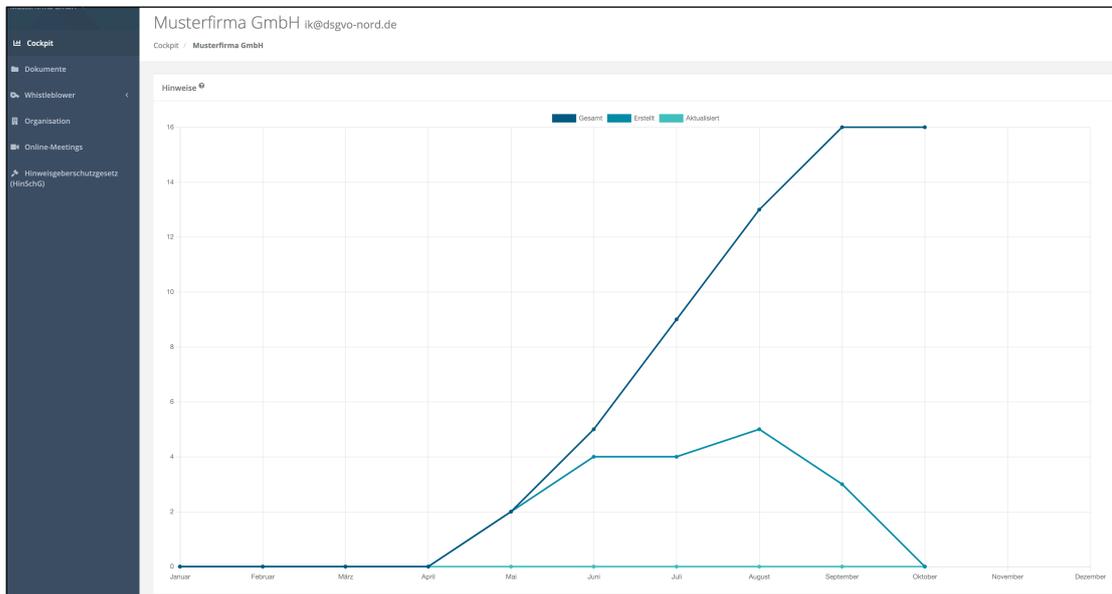
- Ein Benutzer kann alle Meldungen sehen und bearbeiten, dazugehörige Dokumente sowie Notizen einstellen und löschen.
- Auch Benutzer werden über eingehende Meldungen informiert.
- Wenn eine Person eine Meldung über den Meldekanal einreicht, kann sie dies anonym oder offen tun. Wenn sich jemand dazu entscheidet, seine Identität preiszugeben, muss sichergestellt werden, dass die personenbezogenen Daten sicher und geschützt sind.
- Der Benutzer hat Zugriff auf die personenbezogenen Daten, die im Zusammenhang mit den offenen Meldungen gespeichert werden.

### Nur Lesen

- Ein Leser kann alle Meldungen sehen, aber nicht bearbeiten.
- Ein Leser kann bei Meldungen interne Notizen machen und Dokumente für die interne Fallbearbeitung hochladen.
- Ein Leser kann zum Benutzer für einzelne Meldungen gemacht werden und kann dann dort Bearbeitungen vornehmen.

## Interne Auswertungen

Über das „Cockpit“ können Analysen zu Berichtskategorien, Bearbeitungszeiten und anderen Themen eingesehen werden.



Startseite im Cockpit

### 3.2 Technische Grundlagen

Datenschutz entsprechend der DSGVO und der deutschen gesetzlichen Regelungen sind für die dsgvoNORD GmbH ebenso essenziell wie die IT-Sicherheit. Aus diesem Grund haben wir die Lösung in Deutschland entwickelt und mit der Hetzner GmbH einen Cloud-Anbieter gefunden, der unseren höchsten Ansprüchen nach fortschrittlicher IT-Sicherheitsarchitektur vollkommen entspricht. Dazu legt die Hetzner GmbH in gleicher Weise wie hinweis.de großen Wert auf Einhaltung des deutschen Datenschutzstandards.

Die Entscheidung darüber, wie viele Personen Zugriff auf das System erhalten, liegt beim jeweiligen Unternehmen. Jedoch empfehlen wir, den Personenkreis im Unternehmen sehr klein zu halten; bei ca. 1.000 Mitarbeitern sollte es nicht mehr als drei bis fünf Nutzerzugänge geben. Diese Personen werden vom Administrator angelegt und sollten sich stets über eine Zwei-Faktor-Authentifizierung (wie bei einem Online-Girokonto) einloggen, bevor sie Zugriff auf Meldungen erhalten.

### 3.3 Zertifizierungen des Dienstleisters

Das hinweis.de Meldesystem wird bei der Hetzner GmbH gehostet und hat dadurch das Sicherheitsniveau erster Klasse.

Mit folgenden Zertifikaten ist die Hetzner GmbH ISO-zertifiziert:

- ISO 9001 (Qualitätsmanagement)
- ISO 27001, ISO 27017, ISO 27018 (IT-Security)

### **Sprachliche Anforderungen und Einhaltung von Best Practices, Normen und Standards**

Sowohl unsere Programmierer als auch alle Service-Mitarbeitenden leben und arbeiten in Deutschland und sprechen Deutsch als Muttersprache.

Die Erbringung der Leistung erfolgt in vollem Umfang der geforderten Standards, Güte und Normen, insbesondere dem jeweils aktuellen Stand der Technik und unter Verwendung der Festlegungen der jeweils relevanten DIN- und ISO-Normen, gemäß den Standards der IT Infrastructure Library (ITIL), gemäß den BSI-Standards, gemäß den Standards des Project Management Institute (PMI).

## **3.4 Betriebs- und Servicezeiten**

### **3.4.1. Betriebszeit**

Das hinweis.de Meldesystem hat folgende Betriebszeit: 365 Tage à 24 Stunden. Wir gewähren eine 99,8%-ige Erreichbarkeit.

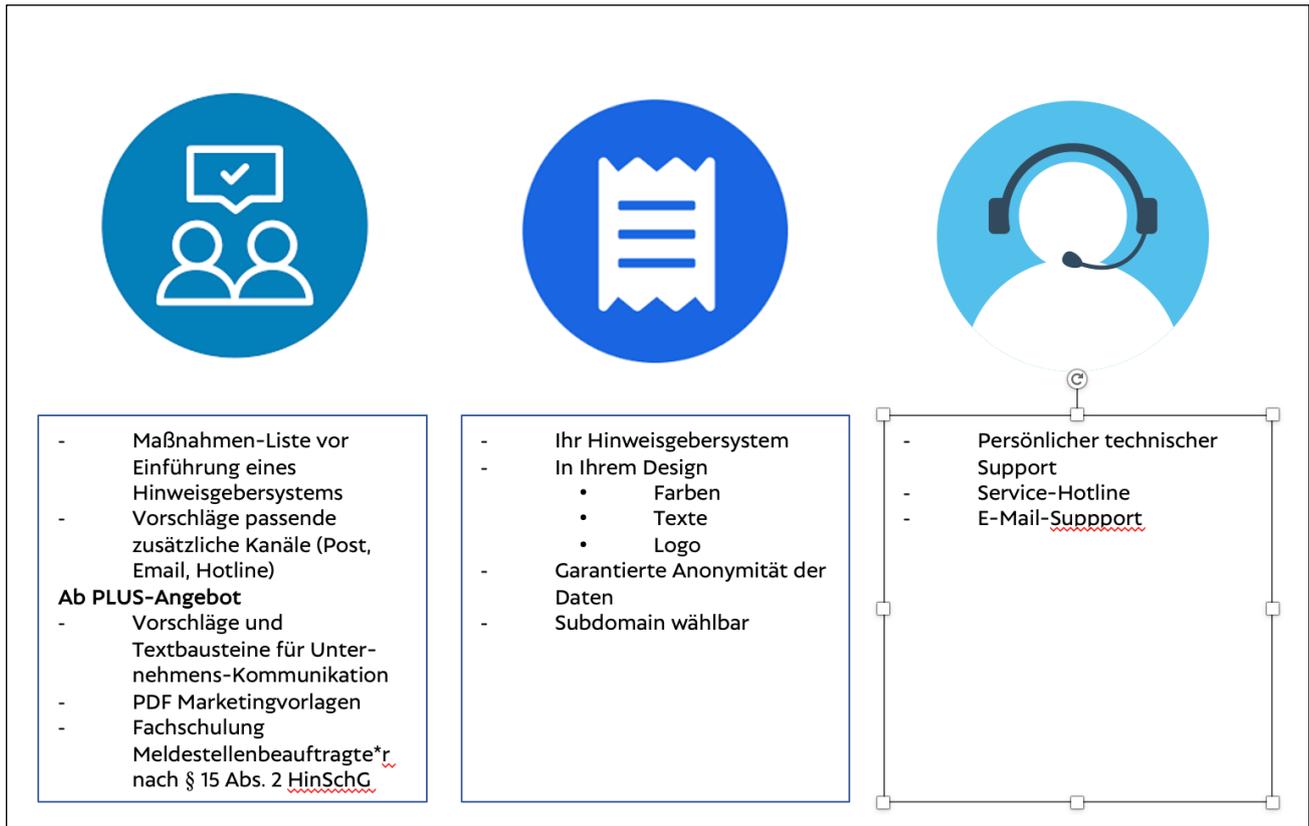
### **3.4.2. Servicezeit**

Die Services unseres Kundenservice stehen Ihnen montags bis freitags von 09:00 Uhr bis 16:00 Uhr zur Verfügung. Die Feiertagsregelung ist auf Grundlage des Bundeslands Schleswig-Holstein vereinbart.

## **3.5 Wartungsfenster**

Regelmäßig wird eine Reihe von kleineren Updates/Patches veröffentlicht. Die Ausfallzeiten durch diese kleineren Updates/Patches sind für den Lizenznehmer nicht bemerkbar. Die Implementierung von kleineren Updates/Patches wird nicht im Voraus kommuniziert.

hinweis.de stellt sicher, dass die Betriebszeit mindestens 99% beträgt. Der Verfügbarkeitsprozentsatz wird pro Kalenderquartal berechnet.



Die dsgvoNORD GmbH entwickelt hinweis.de kontinuierlich weiter und fügt neue Funktionalitäten ohne Mehrkosten für die Kunden hinzu. hinweis.de wird u.a. durch den kontinuierlichen allgemeinen Dialog mit den Anwendern der Lösung zur Entwicklung neuer Funktionalitäten inspiriert. Die dsgvoNORD GmbH priorisiert, inwieweit und in welcher Reihenfolge neue Funktionalitäten implementiert werden.