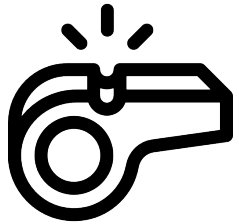
ETHIKBERICHT PROLICHT
2022

PROLICHT GmbH | Götzens

23. Februar 2023

INHALTE ETHIKBERICHT 2022

ETHIK UND
ETHIK-AWARENESS



WHISTLEBLOWING

KORRUPTION

INFORMATIONS-
SICHERHEIT

ETHICAL CONDUCT MAKES A DIFFERENCE

ETHIK

UNSERE WERTE

aus dem PROLICHT Ethik- und Verhaltenskodex

Ein wichtiger Aspekt der fast 30jährigen Erfolgsgeschichte von PROLICHT ist die starke und auf Nachhaltigkeit ausgerichtete Unternehmenskultur. Sie basiert auf der Einhaltung von Gesetzen sowie einem fairen und ethischen Verhalten gegenüber allen Anspruchsgruppen wie Kunden, Mitarbeitern, Geschäftspartnern, Mitbewerbern und Behörden und führt zu unserem ausgezeichneten Image in der Gesellschaft.

P PRIVACY
Wir achten auf Datenschutz

R RESPECT
Wir respektieren einander

O ORGANISATION
Wir achten auf das Unternehmen

L LOYALTY
Wir legen hohen Wert auf Loyalität und treten ein gegen Bestechung und Vorteilsnahme

I INNOVATION
Wir sind Innovationsgetrieben

C CLIMATE PROTECTION
Wir achten auf einen nachhaltigen Umgang mit der Natur

H HUMANITY
Wir setzen Aktionen zum Schutz unserer Mit-Menschen

T TRANSPARENCY
Wir stehen für maximale Transparenz, kämpfen für Ehrlichkeit und vermeiden Interessenskonflikte

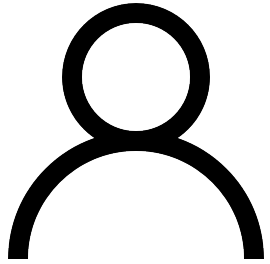
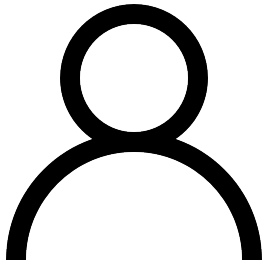
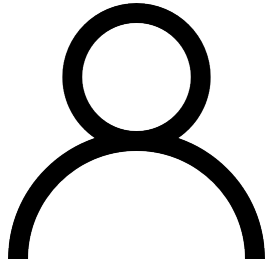
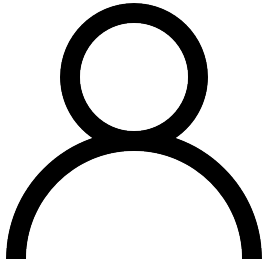
ETHIK BEI PROLICHT

- Hoher Stellenwert von Geschäftsethik. Die Geschäftsleitung, alle Führungskräfte und Mitarbeiter leben und handeln nach diesen Werten.

- Alle Geschäftsprozesse stehen im Einklang mit den „Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte (UNGP)“.

- Mitarbeiter*innen werden laufend für die Themen aus dem PROLICHT Ethik- und Verhaltenskodex geschult und sensibilisiert.

KPI Ethik-Awareness: Mitarbeiter*innen zum Thema Ethik geschult

2021	2022	Ziel 2024	Ziel 2030
			
17%	35%	80%	100%

GOALS ETHIK AWARENESS 2024

PROLICHT

SCHULUNG AWARENESS

- Weitere bestehende Mitarbeiter*innen und neue Mitarbeiter*innen zum Thema Ethik schulen

AWARENESS

- Min. 2x Mitarbeiterinformation von der Geschäftsführung zum Thema Ethik (Video, Newsletter, ...)

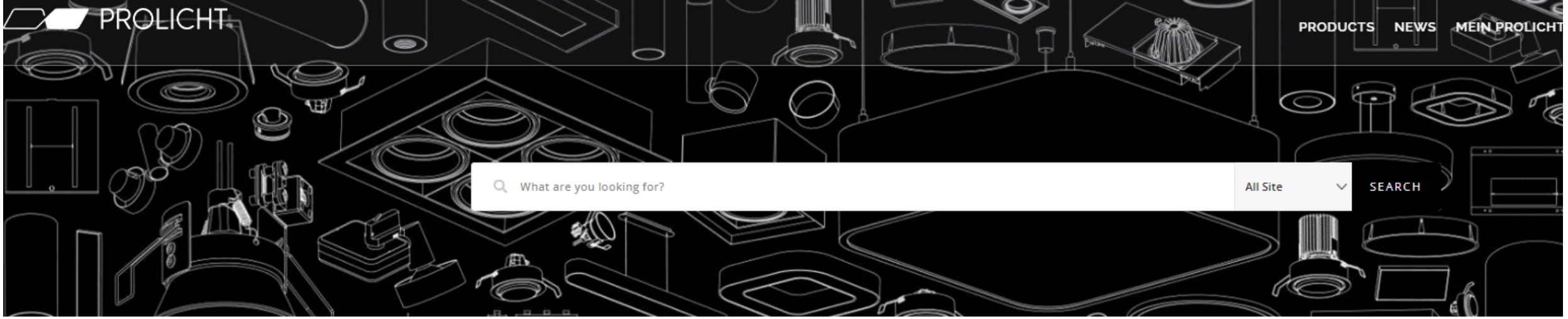
Kennzahl	2020	2021	2022	Ziel 2024	Ziel 2030
Anzahl geschulte Mitarbeiter zum Thema Ethik	0	17%	35%	80%	100%

ETHICAL CONDUCT MAKES A DIFFERENCE

WHISTLEBLOWING

WHISTLEBLOWING BEI PROLICHT
HinweisgeberInnenschutzgesetz - Umsetzung der EU-Whistleblowing-Richtlinie

- Whistleblowing bietet die Möglichkeit, Verstöße im Unternehmen zu melden.
- Das Österreichische HinweisgeberInnenschutzgesetz (HSchG) verpflichtet auch Unternehmen zur Einrichtung interner Meldekanäle, damit Hinweisgeber vertraulich an diese (Verdachtsmomente über) Verstöße melden können.
- Diese Hinweisgeber werden durch das HSchG besonders geschützt.
- Meldekanal wurde bei PROLICHT bereits in Q2/2021 eingeführt



Whistleblowing

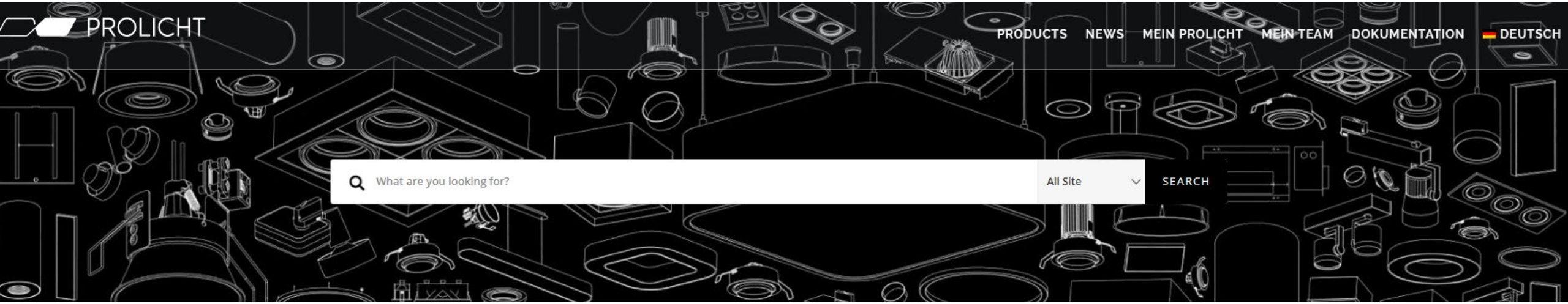
Was ist Whistleblowing?
Unter Whistleblowing versteht man das Melden von Missständen und Vorfällen in einem Unternehmen. Du hast die Möglichkeit, beispielsweise Informationen über Korruption, Betrug oder sonstige illegale Tätigkeiten innerhalb des Unternehmens über unseren sichern Kanal zu melden (siehe Box unten). Wir sind dankbar um jede Meldung!

Welche Verstöße können gemeldet werden?
Folgende Verstöße gegen nationales und Unionsrecht fallen in den Anwendungsbereich der Richtlinie:
- Vorbeugung, Verhinderung und Bekämpfung strafbarer Handlungen um Bereich der Korruption
- Öffentliches Auftragswesen
- Finanzdienstleistungen, Finanzprodukte und Finanzmärkte sowie Verhinderung von Geldwäsche und Terrorismusfinanzierung
- Produktsicherheit und -konformität
- Verkehrssicherheit
- Umweltschutz
- Strahlenschutz und kerntechnische Sicherheit
- Lebensmittel- und Futtermittelsicherheit, Tiergesundheit und Tierschutz
- Öffentliche Gesundheit
- Verbraucherschutz
- Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen

ACHTUNG! Persönliche Missstände wie Mobbing oder Belästigung fallen nicht in den Anwendungsbereich des Whistleblowing-Verfahrens (Siehe unten).

Möchtest du mehr über das Thema Whistleblowing erfahren oder bist du unsicher ob du einen Vorfall melden sollst? Dann sieh dir den Abschnitt „FAQs zum Thema Whistleblowing" weiter unten an.

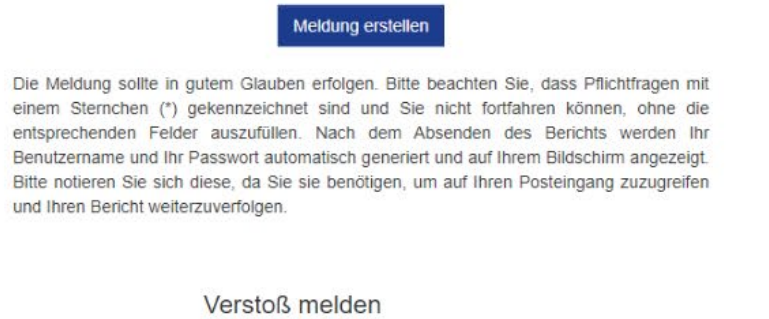
PROLICHT



Erstellen einer Meldung

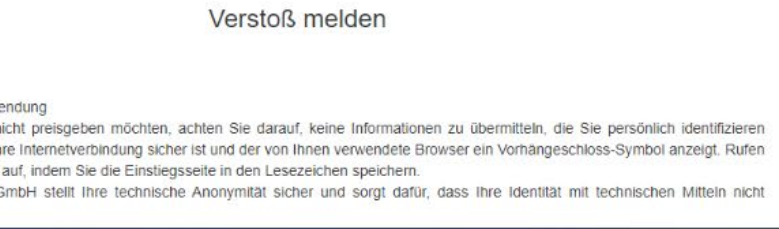
1. Meldung erstellen

Mit einem Klick auf https://prolicht.trusty.report/ öffnet sich der sichere und vertrauliche Meldekanal von PROLICHT. Hier hast du die Möglichkeit, Verstöße oder Missstände im Unternehmen zu melden.
Sobald du die Website aufgerufen hast, kannst du deine Meldung einreichen, indem du auf den Button „Meldung erstellen" klickst.



2. Informationen zur Datenverarbeitung

Im nächsten Schritt erhältst du Infos darüber, wie du den Meldekanal sicher nutzen kannst, und wie die von dir übermittelten Daten verarbeitet werden.



3. Verstoß melden

Im folgenden Schritt wirst du gebeten anzugeben, in welchem Land der Verstoß erfolgt ist.

In welchem Land ist der angebliche Verstoß erfolgt? *

Österreich

Zurück

Weiter

Seite 2 Seite 5

Weiters wirst du gebeten, Informationen darüber zu geben, wann und wo der Verstoß stattgefunden hat, sowie er am Verstoß beteiligt ist bzw. wer ggf. noch Kenntnis von dem Verstoß hat.

Verstoß melden

Für eine erfolgreiche Bearbeitung Ihrer Meldung ist es wichtig, dass Sie so viele Informationen wie möglich zum Thema angeben. Obligatorische Fragen sind mit einem Sternchen gekennzeichnet und Sie können nicht fortfahren, ohne die entsprechenden Felder auszufüllen. Informationen, die in nicht-obligatorischen Feldern bereitgestellt werden, sind sehr willkommen. Sie können diese Felder jedoch überspringen, wenn Sie nicht über das entsprechende Wissen verfügen.

Wann und wo ist der Verstoß aufgetreten?

Personen, die im Verdacht stehen, beteiligt zu sein

Vollständiger Name	Position	Organisation

+

Hat sonst noch jemand Kenntnis von dem Verstoß?

Vollständiger Name	Position	Organisation

+

Bitte beschreiben Sie den Verstoß in Ihren eigenen Worten *

Zum Abschluss der Meldung wirst du gebeten, den Vorfall so detailliert wie möglich in eigenen Worten zu beschreiben.
Hier hast du auch die Möglichkeit, Dokumente anzuhängen.

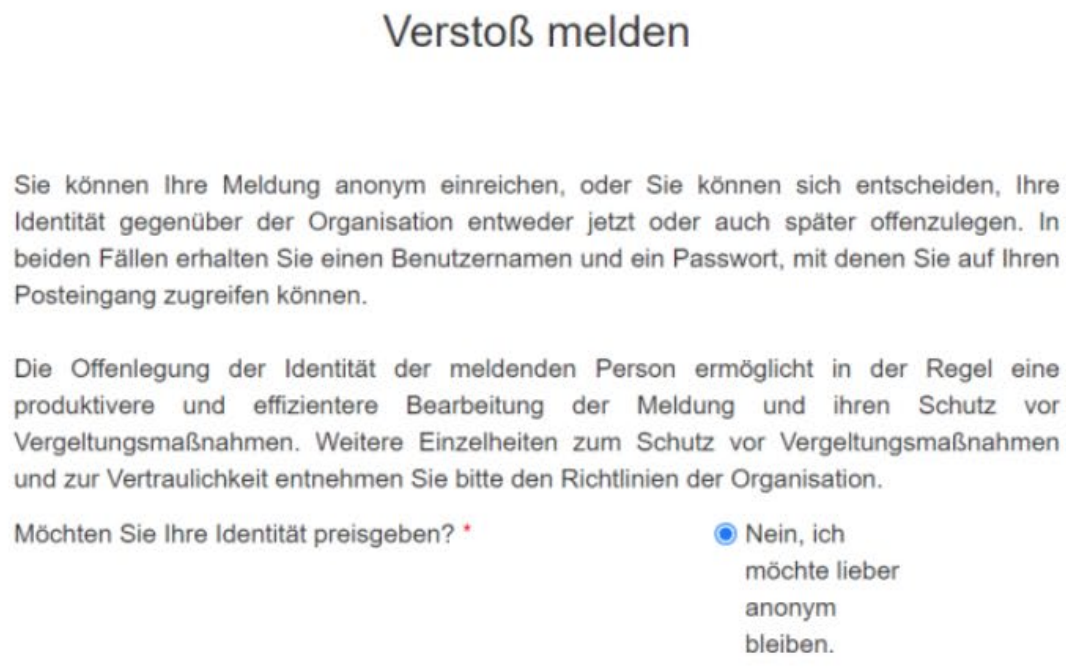
Achtung bei Dokumenten! Wenn du anonym bleiben willst, achte darauf die Metadaten der Dokumente zu überprüfen. Darüber kann deine Identität ermittelt werden. **Hier** gibt's eine Anleitung zum entfernen der Eigenschaften und persönlichen Informationen der Dokumente.

Wenn du dir nicht sicher bist, ob alle Metadaten entfernt sind, kannst du die Dokumente auch in Papierform an PROLICHT (Personalbüro) senden und den Benutzernamen darauf vermerken, den du nach Abschluss der Meldung erhältst.

4. Meldung abschließen

In diesem Abschnitt kannst du entscheiden, ob du die Meldung anonym einreichen möchtest oder deine Identität preisgeben willst.

Mit einem Klick auf „Absenden" wird die Meldung abgeschickt (wenn „anonym bleiben" ausgewählt wurde)



5. Identität preisgeben (optional)

Entscheidest du dich dazu, deine Identität bekannt zu geben, musst du in diesem Schritt die Angaben zu deiner Person ausfüllen.

Mit dem Haken kannst du auswählen, ob du per Mail Benachrichtigungen darüber erhalten möchtest, wenn sich neue Nachrichten in deinem Melde-Postfach befinden (Voraussetzung: E-Mail Adresse angeben)
Achtung! Die Kommunikation bezüglich deiner Meldung erfolgt trotzdem über den Meldekanal.

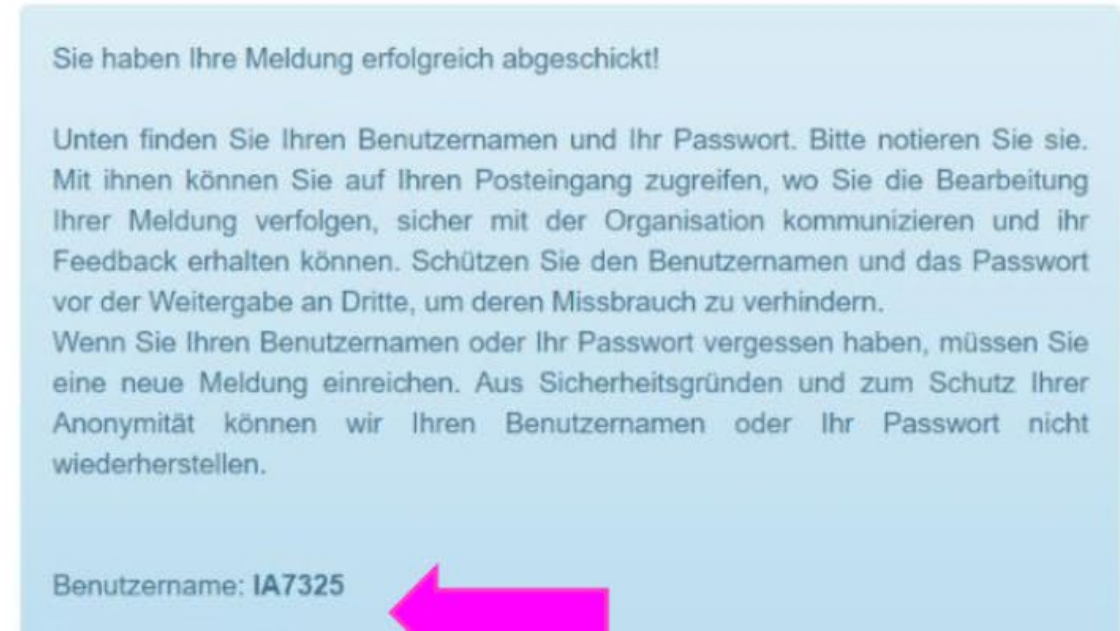
Mit einem Klick auf „Absenden“ wird die Meldung abgeschickt.

6. Meldung abgeschickt

Sobald du die Meldung abgeschickt hast, erscheint folgendes Fenster. Die Anwendung generiert einen Benutzernamen und ein Passwort.

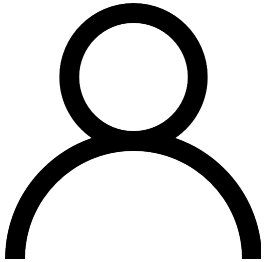
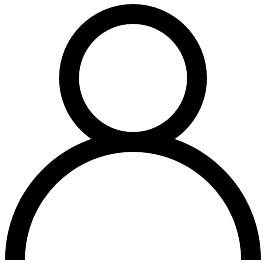
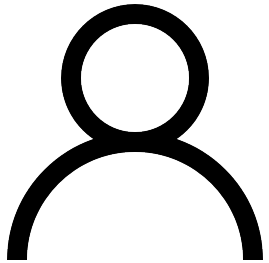
Schreibe dir die Zugangsdaten auf, bewahre sie an einem sicheren Ort auf und gib sie nicht an Dritte weiter!

Du brauchst diese Zugangsdaten um auf dein Postfach zugreifen zu können, in dem die weitere Kommunikation nach der Meldung stattfindet..



KPI Whistleblowing-Awareness:

Mitarbeiter*innen zum Thema Whistleblowing geschult

2022	Ziel 2024	Ziel 2030
		
9%	80%	100%

KPI Monitoring Whistleblowing:
Gemeldete Fälle über Whistleblowing-Kanal

2022	Ziel 2024	Ziel 2030
		
0	0	0
Fälle von Whistleblowing	Fälle von Whistleblowing	Fälle von Whistleblowing

GOALS WHISTLEBLOWING 2024

SCHULUNG	• 80% der Mitarbeiter*innen im Sinne des Whistleblowing-Verfahrens schulen
INFORMATION	• Mitarbeiter*innen min. 2x durch Newsletter über das Thema Whistleblowing informieren
FÄLLE	• Weiterhin 0 zu meldende Missstände

Kennzahl	2020	2021	2022	Ziel 2024	Ziel 2030
Anzahl geschulte Mitarbeiter zu Theam Whistleblowing	0	0	9%	80%	100%
Anzahl Meldungen über Whistleblowing Plattform	0	0	0	0	0

ETHICAL CONDUCT MAES A DIFFERENCE

KORRUPTION

KORRUPTIONSVERMEIDUNG BEI PROLICHT

- PROLICHT verfolgt eine Nulltoleranz-Politik gegenüber Betrug, Korruption, Geldwäsche, sowie wettbewerbsschädigenden Praktiken, die auf unlauteren Wettbewerb abzielen. Wir halten uns bei unseren Geschäftstätigkeiten an alle anwendbaren Gesetze und verbindlichen Vorschriften in allen Ländern, in denen wir tätig sind. Die Führungskräfte auf allen Ebenen informieren sich über den relevanten gesetzlichen und regulatorischen Rahmen und geben die erforderlichen Anweisungen weiter. Unsere Mitarbeiter sind dafür verantwortlich, dass sie die gesetzlichen Erfordernisse in ihrem Arbeitsbereich verstehen und befolgen. Sollten nationale und internationale Vorschriften von unseren internen Vorgaben abweichen, wenden wir, soweit möglich und sinnvoll, den strengeren Maßstab an.

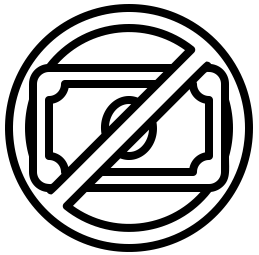
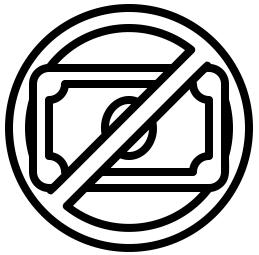
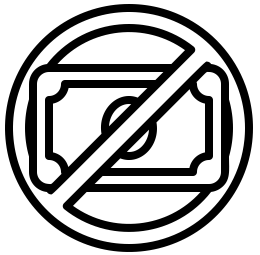
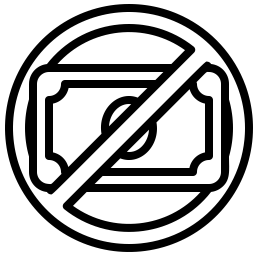
- Überprüfung von neuen und bestehenden Lieferanten durch das PROLICHT Due Diligence Verfahren. Siehe Bericht zur „Nachhaltigen Beschaffung“.

- Schulung und Sensibilisierung der Mitarbeiter*innen im Einkauf und Sales sind in Planung.

- Risikobewertung zum Thema Korruption und Bestechlichkeit erstmalig durchgeführt im Führungskreis von PROLICHT inkl. Planung weiterer Maßnahmen.

KPI Monitoring Korruptionsfälle

Bekannte Fälle zu Korruption

2020	2021	2022	Ziel 2024
			
0	0	0	0
Korruptionsfälle	Korruptionsfälle	Korruptionsfälle	Korruptionsfälle

GOALS KORRUPTIONSVERMEIDUNG 2024

SCHULUNG	• Einkaufs- und Sales-Mitarbeiter*innen in Bezug auf Korruptionsvermeidung sensibilisieren und schulen
PRÜFUNG	• 100% der neuen Lieferanten durch das PROLICHT Due Diligence Verfahren prüfen
RISIKO-BEWERTUNG	• Eine durch den Führungskreis durchgeführte Risikobewertung je Jahr
FÄLLE	• Weiterhin 0 Fälle von Korruption

Kennzahl	2020	2021	2022	Ziel 2024	Ziel 2030
Anzahl Meldungen über Whistleblowing Plattform	0	0	0	0	0
Anzahl geschulte Mitarbeiter zum Thema Korruption/Bestechung	0	0	0	20	100
Anzahl durchgeführte Due Dilicience Bewertung von Lieferanten	0	0	15	25	100
Durchgeführte Risikobwertung zu Korruption/Bestech.	0	0	1	1	1

Geplantes Training zur Korruptionsvermeidung

ZIELE:
Die Mitarbeiter verstehen die Relevanz von Korruptionsprävention im Unternehmen und können planmäßige Korruption und Anfüttern erkennen und höflich unterbinden. Sie wissen außerdem, wie sie sich im Umgang mit Geschenken und Einladungen regelkonform verhalten und welche Warnsignale sie ernst nehmen müssen.
Es gilt Fälle von Bestechung, Bestechlichkeit, Vorteilsannahme und Schmiergeldern zu vermeiden. Mitarbeiter werden auf potenziell gefährliche Situationen vorbereitet und das Training gibt wichtige Verhaltensregeln an die Hand und schützt vor den Folgen korrupten Handelns.

Teilnahme-Voraussetzung:
Aktiver Mitarbeiter / Mitarbeiterin von PROLICHT

Termin der Schulung:
September / Oktober 2023

INHALT:

Korruptionsprävention – worum geht's?
- Korruption: Definition und typische Muster
- Darum muss Korruption bekämpft werden
- Folgen von Korruption

Wege in die Korruption
- Arten von Korruption
- Planmäßiges Anfüttern erkennen
- Bestechung und Bestechlichkeit verhindern

Welche Gesetze regeln Verstöße?
- Korruption ist strafbar
- Nationale Gesetze gegen Korruption
- Internationale Gesetze und Vereinbarungen: FCPA, UK Bribery Act, OECD

Korruptionsprävention in Unternehmen
- Red Flags – hier sollten Mitarbeitende besonders aufmerksam sein
- Umgang mit Einladungen und Geschenken: Was gilt als angemessen und was ist verboten
- Korruption über Dritte verhindern

Risikobewertung zu Korruption und Bestechung

Am 12. Februar 2023 wurde erstmalig im Führungskreis von PROLICHT das Thema Korruption und Bestechlichkeit auf breiter Ebene diskutiert und ein Mix an dezidierten Instrumente zur Risikobewertung für Korruption und Bestechung geplant:

1. Eingänge über die Whistleblower-Plattform
2. Fragebögen: Fragebögen können verwendet werden, um Informationen von Mitarbeitern und Geschäftspartnern zu sammeln, um potenzielle Korruptions- und Bestechungsrisiken zu identifizieren. Diese Fragebögen können auch genutzt werden, um die Einhaltung von Richtlinien und Verhaltensregeln zu überprüfen.
3. Interviews: Interviews können durchgeführt werden, um tiefergehende Informationen von Mitarbeitern und Geschäftspartnern zu sammeln und potenzielle Risikofaktoren zu identifizieren.
4. Datenanalyse: Durch die Analyse von Geschäftsdaten, wie beispielsweise Rechnungen, Auftragsdaten oder Zahlungsströmen, können Unregelmäßigkeiten aufgedeckt werden, die auf Korruption oder Bestechung hindeuten könnten.
5. Due Diligence: Bei der Auswahl von Geschäftspartnern wird eine sorgfältige Überprüfung und Analyse der Geschäftspartner und ihrer Geschäftspraktiken helfen, potenzielle Korruptions- und Bestechungsrisiken zu identifizieren.

<u>Aktuell liegt folgende Risikobewertung (ausgeführt durch den Führungskreis von PROLICHT) vor:</u>

In der Firma PROLICHT gibt und gab es keine Fälle von Korruption und Bestechlichkeit. (vertiefende Analysen sind jedoch geplant). Begründet wird diese Aussage durch folgende Feststellungen:

- Auf der Whistleblower Plattform wurden keine Eingänge vermerkt.
- Die bisherigen Due Diligence Bewertungen der Lieferanten zeigten kein Anzeichen von Bestechlichkeit
- Das Feedback aus den bisherigen Gesprächen im Zuge der Einführung einer Risikobewertung hat keinerlei Anzeichen von Bestechlichkeit und Korruption gezeigt.

ETHICAL CONDUCT MAKES A DIFFERENCE

DATEN- UND INFORMATIONSSICHERHEIT

DATEN- UND INFORMATIONSSICHERHEIT BEI PROLICHT

- Größte Sorgfaltspflicht in Bezug auf personenbezogene Daten.
- Schutz von sensible Unternehmensdaten → PROLICHT Vertraulichkeitsvereinbarung.
- Voller Fokus auf Cyber-Security, Awareness-Schulungsmaßnahmen für Mitarbeiter
- Nur autorisierte Personen kommunizieren auf Social-Media nach außen → (nach Social-Media Kommunikations-Guidelines).
- Zielsetzung für 2023 ist der Abschluss einer Cyber-Security Versicherung. Die notwendigen Voraussetzungen werden hierfür geschaffen.

KPI Monitoring Datensicherheit

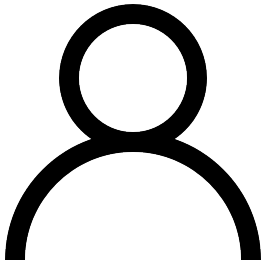
Bekannte Fälle zu nachgewiesenen Fällen von Lücken zur Information- und Datensicherheit

2021	2022	Ziel 2024
0	0	0

KPI Cyber-Security-Awareness:

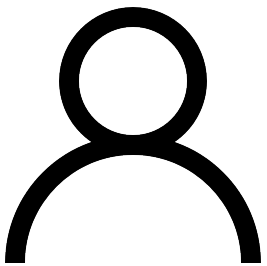
Mitarbeiter*innen zum Thema Cyber-Security geschult

2021



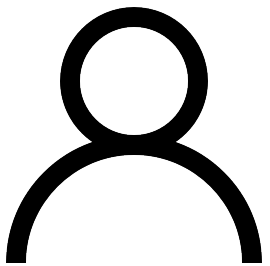
12%

2022



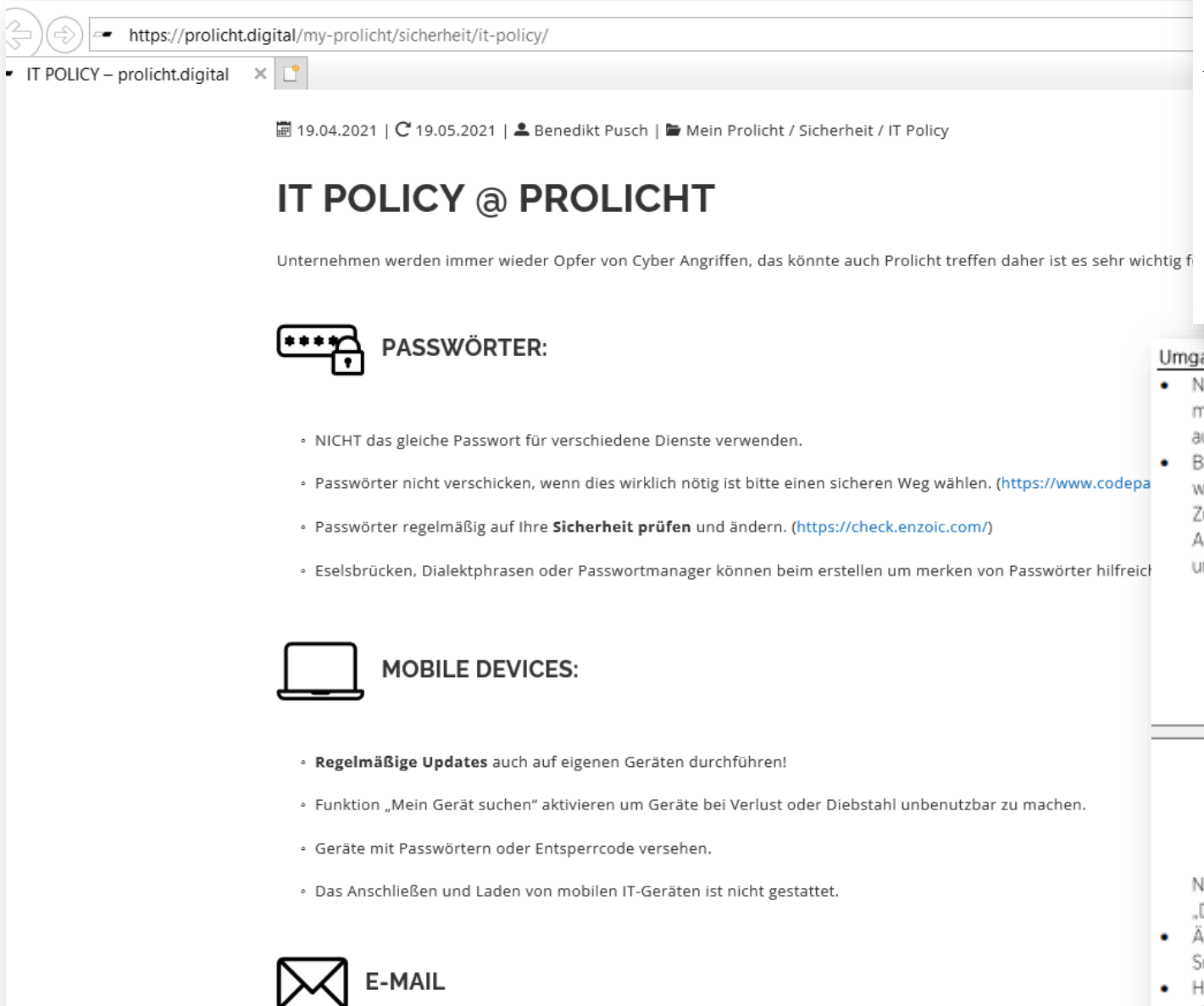
35%

Ziel 2024



100%

Auszug aus der IT Policy im PROLICHT Intranet und der Unternehmensrichtlinie zum Datenschutz



PROLICHT

Anfragen von Kunden, Lieferanten, Partnern zu personenbezogenen Daten:

Bei Anfragen von Kunden und anderen Partnern wie „Wie werden meine personenbezogenen Daten bei Prolicht gespeichert?", Welche Daten speichert Prolicht von mir als Kunde?", „Bitte keinen Newsletter mehr an mich!", „Bitte alle meine Daten im Prolichtsystem löschen!", etc. bitte direkt unseren Datenschutzverantwortlichen Manfred Waldauf (Tel: 05234-33499-70, Email: manfred.waldauf@prolicht.at oder privacy@prolicht.at) informieren. Er wird sich um die Beantwortung dieser Anfragen kümmern.

Emails:

Wir können keine Verantwortung für deine privaten Emails übernehmen. Somit ist aus rechtlichen Gründen die private Nutzung des beruflichen Email Accounts untersagt. Es ist nicht gestattet, auf Werbung, Kettenbriefe etc. zu antworten bzw. diese weiterzuleiten. Dubiose Emails mit unbekannten Absendern dürfen nicht geöffnet werden. Es besteht die Gefahr eines Virenbefalls. Generell unzulässig ist das Versenden oder Verteilen von Material, das von anderen Personen als geschmacklos, Anstoß erregend oder respektlos angesehen werden könnte (zB sexuell eindeutige Bilder, Material das illegale Aktionen befürwortet etc.). Es darf nicht auf von außen kommende Virenwarnungen reagiert werden –hier ist sofort die IT-Abteilung (telefonisch) zu informieren. Gleiches gilt bei Verdacht auf Virenbefall bzw. bei verdächtigen Email-Anhängen, die auf keinen Fall geöffnet werden dürfen.

Durch die Nutzung des Email-Dienstes erklärt der Beschäftigte seine Einwilligung in die Protokollierung

Umgang mit Passwörtern:

- Nutze niemals dasselbe Passwort für alle Portale sondern lege wenigstens für die wichtigsten und meist genutzten Dienste eigene Passwörter an; sonst besteht die Gefahr, dass bei einem Datenklau auch alle anderen Dienste mit deinem Passwort genutzt und missbraucht werden können!
- Baue dir Eselsbrücken, indem du beispielsweise einen Reim oder ein Kinderlied nutzt, das dir immer wieder einfallen wird und von dem du jeweils nur den ersten Buchstaben der einzelnen Wörter nutzt. Zum Beispiel: "Auf der Mauer, auf der Lauer sitzt 'ne kleine Wanze für Facebook." Als Passwort: AdM,adLs'nkWfF. Mit der sich ändernden Endung „für Facebook" kannst du dir leicht Passwörter für unterschiedliche Anwendungen merken.

Seite 3

PROLICHT

Noch ein Beispiel: „Der Ball ist rund & das Runde muss ins Eckige von Prolicht" ergibt das Passwort „DBir&dRmiEvP".

- Ändern deine Passwörter regelmäßig! Dabei reicht schon eine kleine Umstellung oder Ergänzung um Sonderzeichen – nach ca. 3 Monaten wird eine Passwortänderung erzwungen
- Hebe deine Passwörter an einem sicheren Ort zu Hause auf und gib sie nicht per E-Mail, SMS oder

Email an alle PROLICHT Mitarbeiter um „Awareness“ zum Thema IT Security zu schaffen

Von: Hannes Flecker <hannes.flecker@prolicht.at>
Gesendet: Donnerstag, 23. Dezember 2021 10:44
An: PERSONALSTAMM-Götzens; PERSONALSTAMM-Extern
Betreff: SPAM MAIL?

dear colleagues.

a couple of colleagues just got this message.
we are not sure if its trustful at the moment.

please don't open attachments and delete it!

we will check if it's a scam!

thanks to all!

Document

MC Marina Castellano <Marina.Castellano@tomdixon.net>
An Prolicht | Invoic

Document.htm
49 KB

Dear invoices,

I sent you a document.

Kindly find information in th

Lucas Viehweider

Von: Hannes Flecker <hannes.flecker@prolicht.at>
Gesendet: Dienstag, 11. Jänner 2022 10:50
An: PERSONALSTAMM-Götzens; PERSONALSTAMM-Extern
Betreff: Fake Mail again

Dear Colleagues.

Some just got this mail in the screenshot.
I just blocked the sender.

Obviously its fake! Very easy to see on the senders address.
But you know even from trusted senders mails can be fake!

So please be aware with links and attachments you receive. Please DON'T CLICK ON ANY LINKS and delete such mails right away!!!

Von: Hannes Flecker <hannes.flecker@prolicht.at>
Gesendet: Mittwoch, 24. November 2021 09:19
An: PERSONALSTAMM-Extern; PERSONALSTAMM-Götzens
Betreff: Another Fake-Mail Example

Dear Colleagues!

Such mails like down below reach our inboxes more than ever before!
PLEASE DON'T CLICK ON ANY LINKS IN SUCH MAILS AND DELETE THEM RIGHT AWAY!
You can inform us, so we can block the sender. But of course every single day new spammers try their luck to get our response...

Thanks for your help!

21 05:04:25 pm

prolicht.at

Hello pilar.estevez,

Password for pilar.estevez@prolicht.at expires today

11/24/2021 05:04:25 pm

You can change your password or continue using current password.
Keep Using Current Password

Risikobewertung durch Cyber Versicherung

PROLICHT

02.03.2023

ANALYSE ZU CYBER SICHERHEIT

Prolicht GmbH

Cyber Versicherung Cyber Versicherung (AT) Cyber Versicherung

1 2 3 4 5

Allgemeine Informationen

Bitte lesen Sie die Angaben und Fragestellungen sorgfältig durch und beantworten Sie diese wahrheitsgemäß.

Branche:
Bitte wählen Sie die Branche der Versicherungsnehmerin aus:

Select option
Elektrotechnik, Feinmechanik & Optik

Umsatzraster:
Die Versicherungsnehmerin erwirtschaftete im abgelaufenen Geschäftsjahr einen (konsolidierten) Umsatz (in €) von bis

Select option
35.000.000

Börsennotierung:
Ist die Versicherungsnehmerin börsennotiert?

- Ja
- Nein

Tochterunternehmen Ausland:
Die Versicherungsnehmerin hat Tochterunternehmen im Ausland?

Datensicherungen (Regelmäßigkeit):
Existieren regelmäßige Datensicherungen auf separierten Systemen oder Datenträgern? (zum Beispiel NAS,

Select option
Ja, mindestens werktäglich

Datensicherungen (Separierung):
Werden vollständige Offline-Datensicherungen (nicht älter als eine Woche) durchgeführt oder kann auf Back
Active Directory des Unternehmens zugegriffen werden?

- Ja
- Nein

Patch-Management:
Existiert ein geregelter Patch-Management Prozess zur regelmäßigen und durchgehenden Einspielung (inst
(Patches)?

Select option
Ja, mit Einspielung sicherheitskritischer Patches innerhalb von 2 Wochen

IT-Sicherheit

Bitte lesen Sie die Angaben und Fragestellungen sorgfältig durch und beantworten Sie diese wahrheitsgemäß.

Virenschutz:
Wird in Ihrem Unternehmen Virenschutz mit automatischer Aktualisierung eingesetzt?

- Ja
- Nein

GOALS DATEN- UND INFORMATIONSSICHERHEIT 2024

PROLICHT

INFORMATION	• Regelmäßige Information der Mitarbeiter*innen zu aktuellen Phishing-Fällen und Cyber-Security Themen
SCHULUNG	• 100% der neuen Mitarbeiter*innen unterschreiben die PROLICHT DSGVO-Richtlinie
OPTIMIERUNG	• Laufende Optimierung der Systeme im Bereich Cyber-Security und Abschluss einer CyberSecurity Versicherung
RISIKO-BEWERTUNG:	• Eine durch den Führungskreis durchgeführte Risikobewertung je Jahr

Kennzahl	2020	2021	2022	Ziel 2024	Ziel 2030
Anzahl geschulte Mitarbeiter zum Thema CyberSecurity	0	12%	35%	100%	100%
Fälle von Informationssicherheitsvorfällen	0	0	0	0	0
Voraussetzung geschaffen, damit Versicherung möglich	nein	nein	nein	ja	ja
Durchgeführte Risikobwertung zu Daten- und Informationssicherhe	0	0	1	1	1

Risikobewertung zu Daten- und Informationssicherheit

Die Cyber-Attacken auf unsere Mitbewerber im Jahr 2022 haben den Führungskreis von PROLICHT dazu bewegt, dem Thema Daten- und Informationssicherheit noch mehr Aufmerksamkeit zu schenken. Das Thema wurde breit diskutiert und ein Mix an Instrumente zur Risikobewertung für Daten- und Informationssicherheit geplant:

1. Eingänge über die Whistleblower-Plattform
2. Fragebogen Cyber-Security als Standortbestimmung, um Angebote von Cyber-Versicherung zu erhalten. Diese Analysen durch mehrere Dritte (Versicherungsgesellschaften) sollen vor Betriebsblindheit schützen. Aus den Ergebnissen können Verbesserungsmaßnahmen abgeleitet werden. Im Jahr 2023 ist der Abschluss einer Versicherung vorgesehen.
3. Interviews: Interview mit dem DSGVO Beauftragten von PROLICHT könnten wichtige Erkenntnisse bringen.
4. Datenanalyse: Analyse der Fishing Emails, Cyber-Angriffen, Firewall-Protokollen, etc.

<u>Aktuell liegt folgende Risikobewertung (ausgeführt durch den Führungskreis von PROLICHT) vor:</u>
In der Firma PROLICHT gab es bisher einen (nicht bestätigten) Verdacht auf Cyber-Crime. Somit gibt und gab es bei PROLICHT keine Lücken in der Daten- und Informationssicherheit: Begründet wird diese Aussage durch folgende Feststellungen:

- Auf der Whistleblower-Plattform wurden keine Eingänge vermerkt.
- Das Interview mit dem DSGVO Beauftragten von Prolicht ergab kein wesentliches Risikopotenzial.
- Der Analysefragebogen durch die Versicherungen brachte eine sehr positiv Rückmeldung und wenig Risikopotenzial in Bezug auf Cyber-Security. Tipps zur Verbesserung sind:
  - ✓ 2-Faktor-Authentifizierung
  - ✓ 4-Augenprinzip bei Überweisungen von höher EURO 25.000
  - ✓ Trennung der IT-Infrastruktur von Produktion und Office (Netzwerksegmentierung/VLAN), etc.
- Die Bemühungen und das Investment im IT Infrastruktur Team sind sehr hoch.
- Die Awareness der Mitarbeiter ist sehr hoch. Die laufenden Informationen zur Sensibilisierung helfen. Die IT-Policy von PROLICHT wird geschult und von den Mitarbeitern gelebt.

ETHICAL CONDUCT MAKES A DIFFERENCE

DANKE!