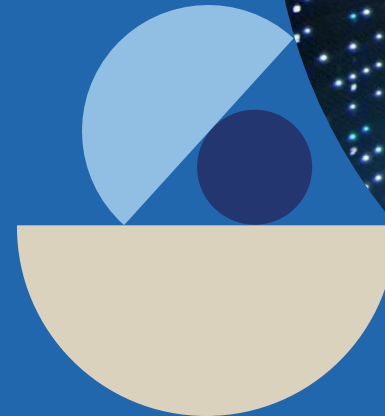


Vorgehensweise zur Erfüllung der “neuen” Obliegenheit

«Durchführung von Schulungen zur Sensibilisierung
hinsichtlich der Themen IT-Sicherheit und Datenschutz»
(Ziffer 6.9.1.2 Absatz c)

Juni 2025



„Neue Obliegenheit“ ...

... die Sicherstellung und regelmäßige Durchführung von präventiven Schulungen zur Sensibilisierung hinsichtlich der Themen IT-Sicherheit und Datenschutz bzw. Grundlagen des Phishings war bislang auch schon eine **wichtige Voraussetzung für den Versicherungsschutz**, wurde bisher jedoch im Rahmen der Risikofragen abgefragt. Ab jetzt wird diese Thematik aufgrund der Änderung des Zusammenarbeitsmodells mit Perseus in die Obliegenheiten / Pflichten im Versicherungsfall verlagert.

Idealtypischer Verlauf – Erfüllung der Präventionspflicht

„Durchführung von Schulungen zur Sensibilisierung hinsichtlich der Themen IT-Sicherheit und Datenschutz“

150 Jahre



Neukundengeschäft Firmen CyberSchutz*

Aufklärung des Kunden im 1. Gespräch, dass Sicherstellung der regelmäßigen Durchführung von präventiven Schulungen eine **wichtige Voraussetzung** für den Versicherungsschutz ist.

Kunde/Interessent hat bereits eine Lösung dafür

Angebotserstellung mit Hinweisblatt auf Obliegenheit

Vertragsabschluss



Kunde / Interessent hat noch **keine** Lösung dafür

Angebotserstellung mit Hinweisblatt auf Obliegenheit und Vertragsabschluss

Zweimonatige Frist zur Erfüllung der neuen Obliegenheit seitens Neukunden

Empfehlung direkt bei Vertragsabschluss:
Perseus Online-Portal für Cybersicherheit
(www.perseus.de/zurich/)

* Dies gilt auch für Bestandskunden, die in der Vergangenheit noch keinen Awareness-Baustein über Zurich / Perseus abgeschlossen haben.

Details zur Erfüllung der „neuen“ Obliegenheit: „Durchführung von Schulungen zur Sensibilisierung hinsichtlich der Themen IT-Sicherheit und Datenschutz“



Durchführung von Schulungen

- 1x jährlich verpflichtend durchgeführte Schulungen zur Sensibilisierung
- hinsichtlich der Themen IT-Sicherheit und Datenschutz
- für **alle Mitarbeitende**, die Zugriff auf das Computersystem des Versicherten haben



Fristen zur Durchführung von Schulungen

- Sicherstellung der Schulung **spätestens 2 Monate nach Versicherungsbeginn** bzw. Durchführung **innerhalb von weiteren 6 Monaten**.
- In den anschließenden Versicherungsperioden ist die Schulung **spätestens 6 Monate nach Beginn der neuen Versicherungsperiode** durchzuführen.



Neu hinzukommende Mitarbeitende

Sicherzustellen, dass neu hinzukommende Mitarbeitende mit Zugriff auf das Computersystem des Versicherten die Schulung **spätestens 3 Monate nach ihrem Eintritt** absolvieren, sofern zu diesem Zeitpunkt bereits eine Pflicht zur Durchführung der Schulung bestand.



Inhalte der Schulungen

Grundlagen des Datenschutzes - insbesondere

- rechtliche Grundlagen gemäß EU-Datenschutz-Grundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG)
- Verarbeitung von Daten
- Verarbeitung personenbezogener Daten (z.B. Kunden- und Lieferantendaten)
- Grundsätze der Datenspeicherung (Sparsamkeit, Erforderlichkeit, Zweckbindung, Transparenz, Einwilligung des Betroffenen)

Grundlagen der Cybersicherheit – insbesondere

- zur Authentifizierung (z.B. sichere Passwörter, Relevanz von 2-Faktoren-Authentifizierung)
- Systemsicherheit (Relevanz von Sicherheits-Updates, Antiviren-Software und Firewalls)

Grundlagen des Phishings

- Regelmäßige Überprüfung der Mitarbeiterkenntnisse durch Phishing-Simulationen