



# SOFTWARELÖSUNG FÜR INFORMATIONSSICHERHEIT & DATENSCHUTZ

## AUF EINEN BLICK:

- Integriertes Managementsystem für Informationssicherheit und Datenschutz, das bei relevanten Zertifizierungen unterstützt
- Einfache Integration und Pflege von Normen und Standards (z.B. ISO 27001, ISO 27019, ISO 27701, NIST, B3S, IT-Sicherheitskatalog)
- Aussagekräftige Dashboards und Reportings
- Abbildung von internen Audits und Self-Assessments
- Revisions sichere Datenhaltung und Historisierung
- Modernes, intuitives Bedienkonzept
- Kurze Einführungszeit durch hohe Standardisierung

# Informationssicherheit und Datenschutz transparent abbilden und effizient verwalten

Unsere Softwarelösung R2C\_SECURITY bildet zwei sicherheitsrelevante Ansätze in einer integrierten Lösung ab. Mit der Anwendung information security können Sie Ihr Informationssicherheitsmanagement (ISMS) professionell organisieren und dokumentieren; die Lösung data protection unterstützt Sie bei der Umsetzung der EU-Datenschutzgrundverordnung.

Wir lassen Ihnen die Wahl: Beginnen Sie mit der Implementierung eines Informationssicherheitsmanagementsystems oder mit der Umsetzung der Anforderungen aus der EU Datenschutz-Grundverordnung oder verwenden Sie nur eines der beiden Elemente.



## Informationssicherheit

Mit der ISMS-Lösung von R2C\_SECURITY steht Ihnen ein effizientes, normenoffenes, auf Ihre Informationssicherheitskonzepte abgestimmtes Werkzeug zum Management Ihrer ISMS-Prozesse zur Verfügung, um Vorgehensweisen und Maßnahmen zur Informationssicherheit zu initiieren, durchzuführen, diese zu überwachen sowie fortlaufend zu prüfen und verbessern. Das ISMS von R2C\_SECURITY unterstützt Sie in allen Phasen des Prozesses, von der Auswahl der relevanten Normen bis hin zur zertifizierungsfähigen Organisation.

## DIE WICHTIGSTEN FEATURES IM ÜBERBLICK

### ORGANISATIONSVERWALTUNG

R2C\_SECURITY ist ein mandantenfähiges System. Die Organisationsstruktur kann über die Mandantenhierarchie abgebildet werden, um den Geltungsbereich des ISMS für die Aufbauorganisation abzubilden. Durch die Mandantenfähigkeit kann eine beliebig tief gestaffelte Organisationsstruktur abgebildet werden.

### ANFORDERUNGSMANAGEMENT

R2C\_SECURITY ist ein normenoffenes System. Die Software ermöglicht das Arbeiten nach den Anforderungen von nationalen und internationalen Normen und Standards, z.B. ISO 27001, 27002, 27005, 27019, 27701, IT-Grundschutzkatalog, B3S, BAIT, VAIT. Weitere Normen, Branchenanforderungen, gesetzliche Vorgaben, interne Richtlinien und unternehmenseigene Standards können ganz einfach integriert und verwaltet werden. Der Anwendungsbereich, d.h. welche Normen, Vorgaben und Richtlinien für das ISMS Anwendung finden, kann einzeln für die Mandanten festgelegt werden.

### UNTERNEHMENSKRITISCHE WERTE VERWALTEN & ANALYSIEREN

- Verwaltung von Geschäftsprozessen und Assets beliebigen Typs, wie z.B. Informationen, Anwendungen, IT-Systeme, Infrastruktur, Gebäude, Räume, Personal
- Abbildung von Geschäftsprozess- und Assethierarchien in beliebiger Tiefe
- Durchführung von Schutzbedarfsanalysen für die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität unter Einbeziehung von Assets/ Geschäftsprozessen sowie automatische Vererbung des Schutzbedarfs mit konfigurierbarer Vererbungsrichtung
- Weitere Schutzziele und Bewertungsdimensionen können frei definiert und optional eingeschaltet werden
- Aufbau von Verbindungen zu Risiken, Schutzmaßnahmen, Kontrollen, Informationssicherheitsvorfällen, Notfallplänen, Verarbeitungstätigkeiten
- Dashboards, Berichte und Auswertungen zur Überwachung der unternehmens- und zeitkritischen Geschäftsprozesse und Assets



## RISIKOMANAGEMENT

- Erfassung und Dokumentation von Risiken in der Informationssicherheit und Einordnung in frei konfigurierbare Risikokategorien
- Benennung von Verantwortlichkeiten
- Einbindung von individuellen Bedrohungs- und Schwachstellenkatalogen zur Durchführung detaillierter Gefährdungsanalysen
- Durchführung schutzzielbezogener Risikoanalysen mit automatisch geerbter Auswirkung
- Erweiterte Risikobewertung auf Basis von individuellen Gefährdungskatalogen
- Individuelle Betrachtung von Risiken vor und nach der Umsetzung von risikomindernden Schutzmaßnahmen (Brutto/Netto-Betrachtung)
- Festlegung von Risikobehandlungsstrategien (z.B. Vermindern, Vermeiden)
- Aufbau von Verbindungen zu Schutzmaßnahmen, Assets, Geschäftsprozessen, Informationssicherheitsvorfällen
- Dashboards, Berichte und Auswertungen zur Überwachung der Risikosituation

## MASSNAHMENMANAGEMENT

- Erfassung und umfassende Dokumentation von Schutzmaßnahmen, von der Planung und Umsetzung bis hin zur Angemessenheits- und Wirksamkeitsprüfung sowie Kostenerfassung und Terminierung
- Benennung von mehreren Verantwortlichkeiten
- Verknüpfung von Schutzmaßnahmen mit Anforderungen/Controls aus Normen, gesetzlichen Vorgaben, internen Richtlinien und unternehmenseigenen Standards als Basis für GAP-Analysen und Audits
- Aufbau von Verbindungen zu Risiken, Assets, Geschäftsprozessen, Informationssicherheitsvorfällen, Kontrollen, Verarbeitungstätigkeiten
- Versand von E-Mail-Benachrichtigungen zur Erinnerung an die Fälligkeit von Maßnahmen
- Dashboards, Berichte und Auswertungen zur Überwachung des Erfüllungsgrades
- Hochladen von Dokumenten per Drag & Drop
- Schnittstelle auf Excel-Basis für einen unkomplizierten Import & Export (manuell, zeitgesteuert und automatisch)
- Flexible Erweiterbarkeit um kundenindividuelle Eigenschaften (Customizing)

## VORFALLSMANAGEMENT (INCIDENT MANAGEMENT)

- Schnelle Erfassung und umfassende Dokumentation von Informationssicherheitsvorfällen
- Benennen von Vorfallsbearbeitern
- Zuordnung betroffener Geschäftsprozesse und Assets sowie eingetretener Risiken
- Einstufung der Auswirkung auf die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sowie Beurteilung der Kritikalität und entstandener Schäden
- Definition von Schutz-, und Verbesserungsmaßnahmen

## AUDIT

Ein Audit ist ein Instrument des Qualitätsmanagements, das untersucht, ob die festgelegten Schutzziele erreicht sind, die relevanten Sicherheitsanforderungen erfüllt werden und die unternehmenskritischen Werte ausreichend geschützt sind. In R2C\_SECURITY können sowohl interne und externe Audits als auch Selbstprüfungen durchgeführt werden. Welche Normen und Standards, welche Teilbereiche davon oder welche Geschäftsprozesse auditiert werden sollen, kann situationsbezogen entschieden werden.

## EINFACHE BEDIENUNG UND HANDHABUNG GROSSER DATENMENGEN

- **Umfangreiche Listen und Detailansichten** - Die in einer Liste dargestellten Spalten und ihre Reihenfolge können benutzerindividuell angepasst werden. Zudem verfügen Listen über umfangreiche Sortier- und Filtermöglichkeiten, über die nach Elementen in der aktuellen Liste effizient gesucht werden kann. Filterdefinitionen können benutzerspezifisch gespeichert und mit einem Klick auf den Filter aktiviert werden.
- **Einfacher Listen-Export in EXCEL- und CSV-Dateien** - Sämtliche Listen können als Excel- bzw. als CSV-Dateien exportiert werden, um weitere Analysen und Auswertungen auf Basis der exportierten Daten durchzuführen. Exportiert werden alle sichtbaren Elemente der aktuellen Liste mit den Informationen aus den dargestellten Spalten.
- **Volltextsuche** - Die integrierte Suchfunktion ermöglicht eine Volltextsuche nach allen in der Anwendung angelegten Bewegungsdaten und zeigt die Suchergebnisse im Rechtekontext des angemeldeten Benutzers an.
- **Journaleinträge und Änderungskommentare** - Alle durchgeführten Änderungen am aufgerufenen Element, z.B. an einem Asset, werden automatisch journalisiert und können durch den Benutzer zusätzlich beschrieben bzw. konkretisiert werden. So bleiben Änderungen, Entscheidungen und Beschlüsse am Element auch Jahre später stets nachvollziehbar.
- **Drag & Drop für Dokumente** - Dokumente können mittels Drag & Drop in die Anwendung hochgeladen werden.





## Datenschutz

Die EU Datenschutz-Grundverordnung stellt den Datenschutz in der Europäischen Union auf eine einheitliche rechtliche Grundlage. Sie muss bis zum 25. Mai 2018 umgesetzt werden, sonst drohen empfindliche Strafen von bis zu 20 Mio. Euro bzw. 4% des weltweiten Jahresumsatzes.

### DIE WICHTIGSTEN FEATURES IM ÜBERBLICK

#### GEMEINSAME DATENBASIS FÜR DATENSCHUTZ- UND ISMS-MANDANTEN

Die Datenschutz Lösung ist so konzipiert, dass Unternehmen auf die grundlegenden Elemente Geschäftsprozess, Asset, Risiko und Maßnahme aus ISMS-Mandanten zugreifen und sie mit den dokumentierten Verarbeitungstätigkeiten im Datenschutz-Mandanten verbinden können.

Vorteil: Die gemeinsame Datenbasis für Informationssicherheit und Datenschutz ermöglicht die einfache Nutzung von einmal angelegten Daten wie Geschäftsprozessen, Assets (z.B. Informationen, Anwendungen, Infrastruktur, Personal), Risiken und Maßnahmen. Es müssen keine redundanten Daten gepflegt werden.

Geschäftsprozesse, Assets, Risiken, Schutzmaßnahmen sowie weitere grundlegenden Elemente können aber selbstverständlich auch eigenständig für den Datenschutz dokumentiert werden.

#### FÜHREN DES VERZEICHNISSES FÜR VERARBEITUNGSTÄTIGKEITEN NACH ART. 30 EU-DSGVO

Das Verzeichnis der Verarbeitungstätigkeiten ist ein zentraler Bestandteil der EU-DSGVO. Dafür müssen wesentliche Angaben über: die Zwecke der Datenverarbeitung, die Kategorien von betroffenen Personen, personenbezogenen Daten und von Empfängern gemacht sowie die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien aufgezeigt werden.

- Das Datenschutzmanagementsystem bietet Unternehmen und Datenschutzbeauftragten die Möglichkeit, alle datenschutzrelevanten Aspekte strukturiert und komfortabel zu erfassen.
- Die Eingabemaske für die Verarbeitungstätigkeiten kann flexibel um kundenindividuelle Eigenschaften erweitert werden (Customizing).

#### RISIKOMANAGEMENT - AUS SICHT DES DATENSCHUTZES

- Erheben und Durchführen von Risikobeurteilungen aus Perspektive des Datenschutzes (Integration der Datenschutzkriterien in die Bewertung)
- Einbindung von individuellen Bedrohungs- und Schwachstellenkatalogen zur Durchführung detaillierter Gefährdungsanalysen
- Festlegung von Risikobehandlungsstrategien (z. B. Vermindern, Vermeiden)
- Definition von technischen und organisatorischen Maßnahmen (TOMs)
- Aufbau von Verbindungen zu Datenschutz-Folgenabschätzungen, Verarbeitungstätigkeiten, Datenschutzvorfällen, Verfahren (Geschäftsprozesse), Assets

## DURCHFÜHREN EINER DATENSCHUTZ-FOLGENABSCHÄTZUNG NACH ART. 35 EU-DSGVO

Eine Datenschutz-Folgenabschätzung ist die Abschätzung der Folgen von Verarbeitungsvorgängen für den Schutz personenbezogener Daten, wenn die Form der Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (vgl. Art. 35 Abs. 1 DSGVO).

- Unsere Lösung unterstützt Sie bei der Entscheidung über die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung. Diese kann sowohl nur für eine als auch für mehrere Verarbeitungstätigkeiten erstellt werden.
- Die Eingabemaske zur Datenschutz-Folgenabschätzung kann flexibel um kundenindividuelle Eigenschaften erweitert werden (Customizing).

## BERICHTE

- **Verzeichnis von Verarbeitungstätigkeiten**  
Der Bericht „Verzeichnis von Verarbeitungstätigkeiten“ liefert alle von der EU-DSGVO geforderten Informationen auf Knopfdruck und kann auf Anfrage der Aufsichtsbehörde zur Verfügung gestellt werden. Das Verzeichnis kann sowohl aus der Sicht eines Verantwortlichen als auch aus der Sicht eines Auftragsverarbeiters erstellt werden.
- **Datenschutz-Folgenabschätzung**  
Der Bericht „Datenschutz-Folgenabschätzung“ liefert alle von der EU-DSGVO geforderten Informationen auf Knopfdruck und kann zum Beispiel im Rahmen einer Konsultation der Aufsichtsbehörde zum Einsatz kommen.





## Internes Kontrollsystem

Unsere IKS-Lösung in R2C\_SECURITY unterstützt Sie effektiv und zuverlässig bei der Überwachung aller notwendigen Prozesse innerhalb Ihres Unternehmens. Es ermöglicht die Definition von beliebigen Kontrollen zur regelmäßigen Prüfung und Überwachung von Geschäftsprozessen, Assets, Risiken, Maßnahmen, Vorfällen, Verarbeitungstätigkeiten in einer Anwendung.

### DIE WICHTIGSTEN FEATURES IM ÜBERBLICK

#### BESCHREIBUNG UND ZUORDNUNG VON KONTROLLEN

Eine Kontrolle kann umfassend beschrieben und kontrollverantwortlichen Mitarbeitern zugeordnet werden.

#### KONTROLLBESTÄTIGUNG

Für die regelmäßige Durchführung einer Kontrolle kann eine Bestätigungsfrequenz hinterlegt werden. Anhand der eingestellten Bestätigungsfrequenz (z.B. wöchentlich) werden periodisch Kontrollbestätigungen erzeugt, über die der verantwortliche Mitarbeiter die regelmäßige Durchführung der Kontrolle bestätigen und das Kontrollergebnis dokumentieren kann.

#### HINTERLEGUNG VON KONTROLLEN

Kontrollbestätigungselemente werden dem verantwortlichen Benutzer automatisch in seinem persönlichen Aufgabenkorb hinterlegt und können von dort aus zentral verwaltet, bestätigt und um Nachweisdokumente ergänzt werden.

#### GRAFISCHE AUSWERTUNG VON KONTROLLEN

Über eine grafische Auswertung können alle vergangenen und aktiven Kontrollen und Kontrollergebnisse zentral überwacht und nachverfolgt werden.

#### BENACHRICHTIGUNGSFUNKTION

Kontrollverantwortliche Mitarbeiter können zu relevanten Kontrollereignissen benachrichtigt und mit automatisch generierten E-Mails an die Fälligkeit von Kontrollbestätigungen erinnert werden.



## Das bietet Ihnen die Softwarelösung R2C\_SECURITY

### ZENTRALE SOFTWAREEIGENSCHAFTEN

- intuitives, modernes und webbasiertes Bedienkonzept
- einfache Integration in die bestehende IT-Landschaft
- ADFS-Anbindung für ein unternehmens- und netzwerkübergreifendes Single Sign-on (SSO)
- mehrsprachige Benutzeroberfläche
- flexible Anpassung / Erweiterung der Software auf die spezifischen Anforderungen des Unternehmens
- aussagekräftige Dashboards und Reportings
- optimale Prozessunterstützung
- Revisionsicherheit durch Journalisierungs- und Historisierungsfunktion
- umfangreiche Import- und Exportmöglichkeiten, z. B. von Katalogen und Inventardatenbank
- normoffenes System, das bei Zertifizierungen (z.B. ISO 27001 ) unterstützt
- Software made in Germany

### IHRE VORTEILE

- Integriertes Managementsystem für Informationssicherheit und Datenschutz
- Dokumentation des Datenschutzes nach EU-DSGVO
- hohe Akzeptanz der Software durch einfaches und modernes Bedienkonzept
- geringer Einführungsaufwand durch hohe Standardisierung
- rollenbasiertes Berechtigungskonzept (Need-to-Know-Prinzip)
- revisionssichere Dokumentation
- Kundensupport mit Inhouse-Mitarbeitern
- Kontinuierliche Verbesserung und Weiterentwicklung auf Basis von Best-Practice-Ansätzen
- auditorengerechte Abbildung externer und interner Audits
- Punktwerte zur effektiven Einschätzung von Schutzbedarfen und Kritikalitäten

## Die GRC-Cloud für Ihre R2C-Lösung

Schleupen ist der verlässliche Partner, wenn es um GRC-Anwendungen geht. Darum bieten wir unsere Anwendungen R2C\_GRC und R2C\_Security nicht nur **On Premises** an, also bei Ihnen im System installiert, sondern auch in der **Cloud**.

Unsere GRC-Cloud ist immer online, immer verfügbar und voll skalierbar. So nutzen Sie die volle Funktionalität der R2C-Lösungen zu einem geringen Aufwand. Sicherheit hat dabei oberste Priorität. Auch darum werden alle Daten in einem deutschen Rechenzentrum gehostet: Zertifiziert nach ISO 27001.

## IHRE GRC-EXPERTEN SIND FÜR SIE DA!



Wir beraten Sie gerne rund um die Themen Informationssicherheit und Datenschutz. Ebenso haben Sie die Möglichkeit, unsere Softwarelösung in einem kostenlosen Web Seminar anzusehen – sprechen Sie uns an!

 +49 (0)7243 321-4700

 [grc@schleupen.de](mailto:grc@schleupen.de)



[www.schleupen-grc.de](http://www.schleupen-grc.de)