Cortina Consult

Datenschutzbericht

zum Datenschutzprojekt

Berichtszeitraum: 14.06.2021 bis 03.11.2022

NorthRock software GmbH
Hanauer Landstraße 146
60314 Frankfurt am Main

Cortina Consult GmbH
Hafenweg 24
48155 Münster
+49 251 29794740
support@cortina-consult.de
www.cortina-consult.com

Cortina Consult

Inhalt

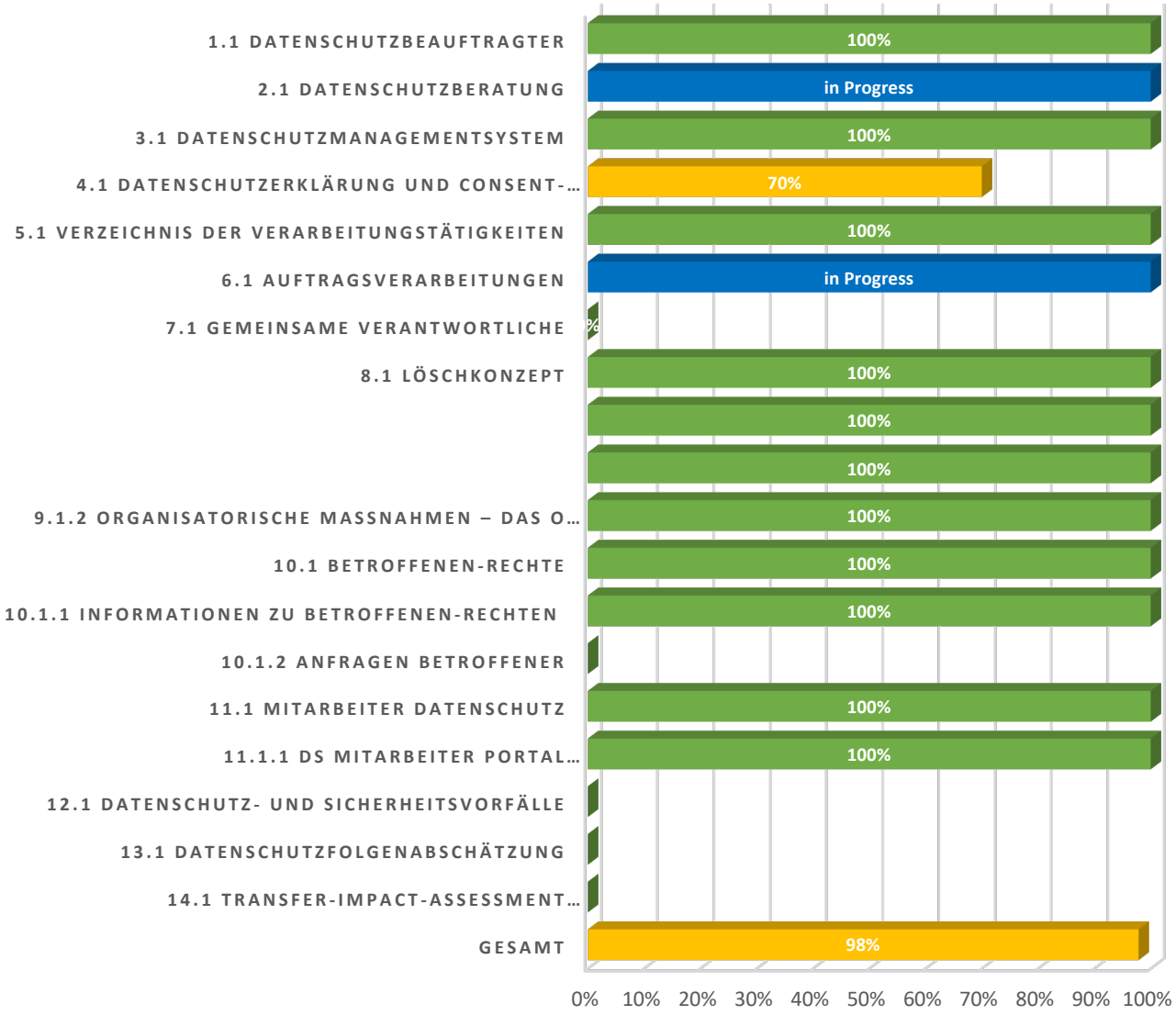
Cortina Consult

Einleitung

Am 14.06.2021 sind wir mit dem gemeinsamen Datenschutzprojekt gestartet. Um Sie über den „Status quo“ des Projekts und weitere, außerhalb des Projekts umgesetzte Tätigkeiten umfassend zu informieren, haben wir Ihnen den nachfolgenden Datenschutzbericht erstellt. Teilweise werden Grafiken und Übersichtslisten zu einzelnen Themengebieten verwendet; diese stammen aus der gemeinsam genutzten Datenschutzsoftware.

Sie erhalten diesen Bericht ab sofort jährlich.

Status-Übersicht – Management-Summary



Datenschutzbeauftragter

Die formale Bestellung des externen Datenschutzbeauftragten ist erfolgt und die Meldung bei der zuständigen Datenschutzbehörde vorgenommen.

Datenschutzberatung

Zur Datenschutzberatung gehören alle Leistungen, die nicht Bestandteil Bereitstellungspauschale sind, wie bspw. Recherchen und Beantwortung individueller Datenschutzanfragen. Die Abrechnung erfolgt gesondert. Nachfolgende Tätigkeiten fallen unter den Begriff der Datenschutzberatung:

Schlüssel	Zusammenfassung	Bearbeiter	Autor	Status
CC-5064	FW: List von E-Mail Attributen für Online AVV	Joshua Tiedtke	Martina Brinkmann	DONE
CC-4489	AVV - Vereinbarung zur Auftragsverarbeitung - 085 - Polystein	Joshua Tiedtke	Martina Brinkmann	IN PROGRESS

2 Vorgänge Aktualisieren

Datenschutzmanagementsystem (DSMS)

Die Basis eines Datenschutzmanagementsystems ist eingeführt worden. Gerade dieser Aspekt muss allerdings stetig fortgeführt werden, da das Thema Datenschutz ein sich ständig weiterzuentwickelnder Prozess bleibt und letztlich nie zum Abschluss kommen kann.

Datenschutzerklärung und Consent-Management (DSE & CMP)

Für jede Form der Online-Präsentation eines Unternehmens (Website, Social-Media-Fanpage, etc.) wird neben dem Impressum eine Information gem. Art. 13 DSGVO benötigt – auch bekannt unter dem Begriff Datenschutzerklärung (DSE). Die DSE informiert über jede Verarbeitung der Website, die keiner Einwilligungspflicht unterliegt. Für alle anderen Verarbeitungen (wie z.B. Google Analytics, YouTube-Integrationen, Google Maps u.w.m.) muss eine Einwilligung eingeholt werden; sinnvollerweise über eine sogenannte CMP (Consent Management Platform).
Da nicht immer gewährleistet werden kann, dass neue Integrationen des Marketings (z.B. Google Ads u.a.) dem Datenschutzbeauftragten gemeldet werden, haben wir ein Monitoring-Tool entwickelt, welches den aktuellen Compliance-Status der Website scannt und in Form eines ausführlichen Ergebnisses ausgibt. Der im Monitoring hinterlegte Ansprechpartner erhält per E-Mail regelmäßig die Information zum jeweiligen Scan-Ergebnis.

Den „Status quo“ der uns bekannten Websites und Social-Media-Fanpages zeigt die Übersichtsliste.

Übersicht

URL	Status der DSE	Status der CMP	Ansprechpartner Monitoring

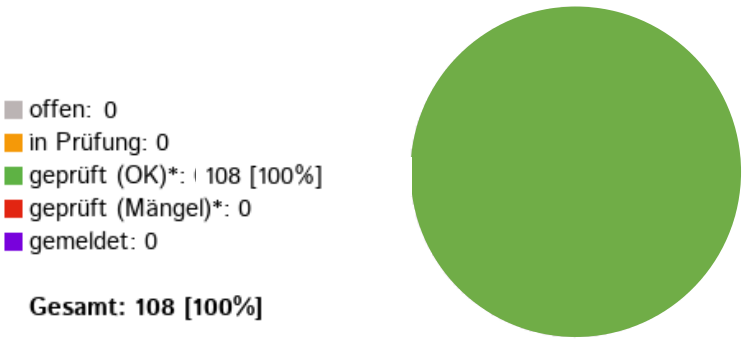
Northrock.software	Geprüft (OK) → Upgrade auf Cloud DSE empfohlen	Geprüft (kleine Mängel)	Leon Bernard
Maintain.de	Geprüft (Änderung notwendig)	Geprüft (Änderung erforderlich)	Leon Bernard

Verzeichnis der Verarbeitungstätigkeiten (VVT)

Gemäß der DSGVO haben alle Unternehmen eine Dokumentations- und Rechenschaftspflicht bezüglich des Umgangs mit personenbezogenen Daten. Für jeden vorhandenen datenschutzrelevanten Prozess sowie das ggfs. damit verbundene IT-System muss ein Eintrag im sogenannten Verfahrensverzeichnis angelegt werden (Art. 30 DSGVO).

Nachfolgende Verfahren wurden im DSMS erfasst, ggfs. geprüft und dokumentiert. Den „Status quo“ der Verarbeitungen zeigen das Diagramm sowie die Übersichtsliste.

Diagramm



Übersicht

Bezeichnung	Status	Letzte Änderung
Besucherverwaltung	Geprüft (OK)	23.03.2022
Presse	Geprüft (OK)	23.03.2022
(Online) Banking	Geprüft (OK)	23.03.2022
Abrechnung Lastschrift	Geprüft (OK)	23.03.2022

Abteilungswechsel	Geprüft (OK)	23.03.2022
Abwesenheit, Urlaub	Geprüft (OK)	23.03.2022
Adresskauf	Geprüft (OK)	23.03.2022
Akquise	Geprüft (OK)	23.03.2022
Aktenhaltung	Geprüft (OK)	23.03.2022
Allgemeine Verwaltung	Geprüft (OK)	23.03.2022
Allgemeiner Netzwerkschutz	Geprüft (OK)	23.03.2022
Analyse und Reporting	Geprüft (OK)	23.03.2022
Anfragen Dritter	Geprüft (OK)	23.03.2022
Angebots-, Auftrags-, Rechnungserstellung	Geprüft (OK)	23.03.2022
App-Entwicklung	Geprüft (OK)	23.03.2022
Aufgabenzuweisung	Geprüft (OK)	23.03.2022
Auftragsabwicklung	Geprüft (OK)	23.03.2022
Auftragsverwaltung	Geprüft (OK)	23.03.2022
Auskunftsverfahren Betroffener	Geprüft (OK)	23.03.2022
Ausschreibungen	Geprüft (OK)	23.03.2022
Backup	Geprüft (OK)	23.03.2022
Beendigung der Beschäftigung	Geprüft (OK)	23.03.2022
Benutzerverwaltung	Geprüft (OK)	23.03.2022
Bestellbericht	Geprüft (OK)	23.03.2022
Bestellwesen	Geprüft (OK)	23.03.2022
Betriebskostenabrechnung	Geprüft (OK)	23.03.2022

Bewerbermanagement	Geprüft (OK)	23.03.2022
Bilder und Videos bei Veranstaltungen	Geprüft (OK)	23.03.2022
Bürokommunikation	Geprüft (OK)	23.03.2022
Controlling	Geprüft (OK)	23.03.2022
CRM-System (Customer-Relationship-Management)	Geprüft (OK)	23.03.2022
Daten an Unternehmensberater	Geprüft (OK)	23.03.2022
Datenaustauschportal	Geprüft (OK)	23.03.2022
Datenträgerentsorgung	Geprüft (OK)	23.03.2022
Device Management	Geprüft (OK)	23.03.2022
Dienstleistung	Geprüft (OK)	23.03.2022
Distribution	Geprüft (OK)	23.03.2022
DMS Dokumentenmanagementsystem	Geprüft (OK)	23.03.2022
Druck- und Kopieraufträge	Geprüft (OK)	23.03.2022
E-Learning	Geprüft (OK)	23.03.2022
E-Mail Archivierung	Geprüft (OK)	23.03.2022
Eingangspost	Geprüft (OK)	23.03.2022
Einstellungsprozess (Mitarbeiter / Azubis)	Geprüft (OK)	23.03.2022
Elektronische Verarbeitung per E-Mail	Geprüft (OK)	23.03.2022
ERP-Software	Geprüft (OK)	23.03.2022
Gehalts- und Lohnabrechnung	Geprüft (OK)	23.03.2022

Groupwaresystem	Geprüft (OK)	23.03.2022
Home-Office	Geprüft (OK)	23.03.2022
Hosting	Geprüft (OK)	23.03.2022
Interessenverwaltung	Geprüft (OK)	23.03.2022
Internet- und Telefonnutzung	Geprüft (OK)	23.03.2022
Intranetnutzung	Geprüft (OK)	23.03.2022
IT-Sicherheit	Geprüft (OK)	23.03.2022
IT-Support (Remote)	Geprüft (OK)	23.03.2022
Kommunikationssysteme (wie z.B. Telefonanlage)	Geprüft (OK)	23.03.2022
Kontaktformular	Geprüft (OK)	23.03.2022
Kontaktverwaltung	Geprüft (OK)	23.03.2022
Kontrolle der Internetnutzung	Geprüft (OK)	23.03.2022
Kunden - Foto und Film	Geprüft (OK)	23.03.2022
Kundenbefragung (anonym)	Geprüft (OK)	23.03.2022
Kundenbetreuung und CRM	Geprüft (OK)	23.03.2022
Kundensupport	Geprüft (OK)	23.03.2022
Lieferantenmanagement	Geprüft (OK)	23.03.2022
Marketingmaßnahmen	Geprüft (OK)	23.03.2022
Messefotos	Geprüft (OK)	23.03.2022
Microsoft 365	Geprüft (OK)	23.03.2022
Mitarbeitergespräche	Geprüft (OK)	23.03.2022
Mobile, Handy, Smartphone-Nutzung	Geprüft (OK)	23.03.2022

Newsletter	Geprüft (OK)	23.03.2022
Notfallkonzept	Geprüft (OK)	23.03.2022
Online Marketing	Geprüft (OK)	23.03.2022
Online Meetings	Geprüft (OK)	23.03.2022
Papier- und Aktenvernichtung	Geprüft (OK)	23.03.2022
Parkplatzzuweisung	Geprüft (OK)	23.03.2022
Personaldatenverarbeitung	Geprüft (OK)	23.03.2022
Personalfragebogen	Geprüft (OK)	23.03.2022
Poststelle	Geprüft (OK)	23.03.2022
Projektmanagement	Geprüft (OK)	23.03.2022
Protokollierung in IT-Systemen	Geprüft (OK)	23.03.2022
QM-Handbuch	Geprüft (OK)	23.03.2022
Qualitätssicherung	Geprüft (OK)	23.03.2022
Rechenzentren	Geprüft (OK)	23.03.2022
Rechnungs-, Mahnwesen & Finanzbuchhaltung	Geprüft (OK)	23.03.2022
Revision, Compliance	Geprüft (OK)	23.03.2022
Schlüsselverwaltung	Geprüft (OK)	23.03.2022
Schulungen, Seminare (Fortbildungen)	Geprüft (OK)	23.03.2022
Social Media Marketing	Geprüft (OK)	23.03.2022
Software-Entwicklung	Geprüft (OK)	23.03.2022
Technische Ausstattung	Geprüft (OK)	23.03.2022
Terminverwaltung	Geprüft (OK)	23.03.2022

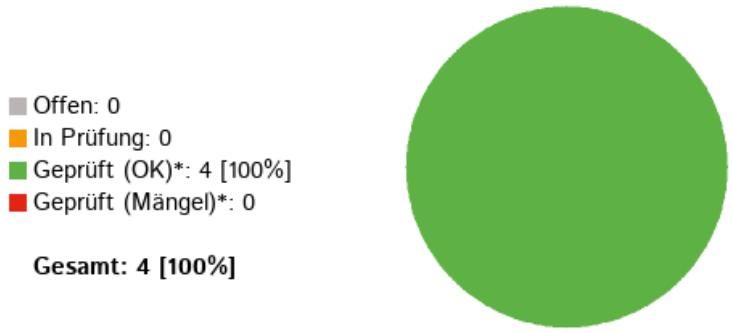
Ticketsystem	Geprüft (OK)	23.03.2022
Überweisungsgeschäft	Geprüft (OK)	23.03.2022
Umgang mit Passwörtern	Geprüft (OK)	23.03.2022
Unternehmenswebsite	Geprüft (OK)	23.03.2022
Veranstaltungen und Events	Geprüft (OK)	23.03.2022
Verbesserungsprozess	Geprüft (OK)	23.03.2022
Vertragsverwaltung	Geprüft (OK)	23.03.2022
Verwaltung Mobilfunkverträge	Geprüft (OK)	23.03.2022
Webshop	Geprüft (OK)	23.03.2022
Websiteauswertung	Geprüft (OK)	23.03.2022
Wirtschaftsauskunft, Bonitätsprüfung, Inkasso	Geprüft (OK)	23.03.2022
WLAN	Geprüft (OK)	23.03.2022
WLAN (Gäste)	Geprüft (OK)	23.03.2022
Zeiterfassungssystem	Geprüft (OK)	23.03.2022
Zugangskontrolle	Geprüft (OK)	23.03.2022
Zugriffskontrolle (Berechtigungskonzept)	Geprüft (OK)	23.03.2022
Zutrittskontrolle	Geprüft (OK)	23.03.2022
Zutrittskontrolle Fremdarbeiter	Geprüft (OK)	23.03.2022

Auftragsverarbeitung (AVV)

Auftragsverarbeitung bezeichnet die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen sogenannten Auftragsverarbeiter (Dienstleister) gemäß den Weisungen des für die Datenverarbeitung Verantwortlichen auf Grundlage eines Vertrages (gem. Art. 28 DSGVO).

Es wurden mit allen uns bekannten externen Dienstleistern, die im Auftrag personenbezogene Daten verarbeiten oder im Rahmen ihrer Dienstleistung auf diese Zugriff haben, entsprechende Vereinbarungen gem. Art. 28 DSGVO abgeschlossen und in das AV-Verzeichnis der Datenschutzsoftware übertragen. Den „Status quo“ der Vereinbarungen zeigen das Diagramm sowie die Übersichtsliste.

Diagramm



Übersicht

Art	Bezeichnung	Firma	Organisationseinheit	Status	Vertragsstatus	
AG	E-Mail Newsletter Dienstleistung	maintain BIO MOTION LAB	Geschäftsführung	geprüft (OK)	AV-Vertrag (Art. 28 DS-GVO)	●
AG	E-Mail Newsletter Dienstleistung	MAINTAIN	Geschäftsführung	geprüft (OK)	AV-Vertrag (Art. 28 DS-GVO)	●
AG	MD-HR App & MD-HR Monitor	MD Elektronik GmbH	Geschäftsführung	geprüft (OK)	AV-Vertrag (Art. 28 DS-GVO)	●
AG	Nextcloud Hosting	MAINTAIN	Geschäftsführung	geprüft (OK)	AV-Vertrag (Art. 28 DS-GVO)	●

Gemeinsam Verantwortliche

Sobald zwei (oder auch mehr) separate Unternehmen gemeinsam über den Zweck und die Mittel der Verarbeitung personenbezogener Daten entscheiden, gelten sie als sogenannte gemeinsam Verantwortliche gem. Art. 26 DSGVO. Für die betreffende Verarbeitung muss in einer Vereinbarung festgelegt werden, wer für welche Verpflichtungen gem. DSGVO, insbesondere gegenüber den Betroffenen, zuständig ist.

Bisher wurden keine Vereinbarungen zur gemeinsamen Verantwortlichkeit zur Prüfung eingereicht. Sollten Ihnen entsprechende Verarbeitungen innerhalb Ihres Unternehmens bekannt sein, teilen Sie uns dies bitte mit.

Löschkonzept

Ein Konzept zur Umsetzung und Einhaltung datenschutzkonformer Löschvorgaben wurde eingeführt, welches alle relevanten Kategorien personenbezogener Daten beinhaltet. Das Löschkonzept dient als zentrales Dokument für die Identifizierung, Konzeptionierung sowie einfache Illustration von Löschfristen.
Die vorhandenen Löschfristen werden zusammen mit der Rechtsquelle, wie z.B. des Bürgerlichen Gesetzbuchs oder des Handelsgesetzbuchs, aufgeführt. Mit Umsetzung der im bestehenden Löschkonzept konzeptionierten Löschvorgaben kommt Ihr Unternehmen dem Prinzip der Datenminimierung des europäischen Gesetzgebers nach: Alle personenbezogenen Daten werden nach Zweckwegfall gelöscht. Sofern gesetzliche Aufbewahrungsfristen einer Löschung entgegenstehen, erfolgt ggfs. eine Sperrung der Daten.

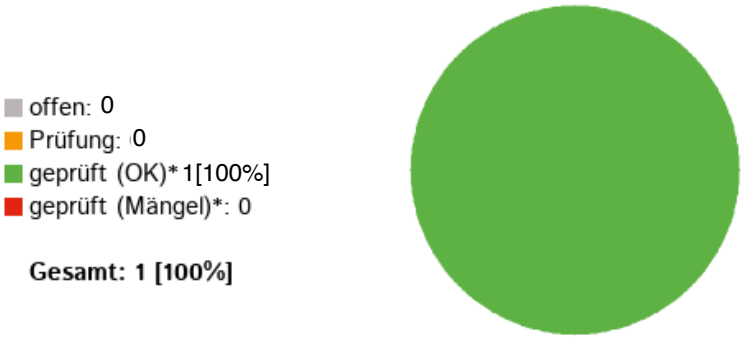
Technische und organisatorische Maßnahmen (TOM)

Technische Sicherheits-Maßnahmen – das T in TOM

Technische Vorkehrungen zum Schutz der Unternehmensdaten (Datensicherheit) sind ein wesentlicher Aspekt zum Schutz personenbezogener Daten (Datenschutz) – die Auswahl adäquater Sicherheitswerkzeuge ist somit ein wesentlicher Baustein der DSGVO. Die praktische Umsetzung dieser Maßnahmen – und damit verbunden die Pflicht zur Dokumentation der getroffenen Vorkehrungen – ergibt sich aus den gesetzlichen Vorgaben an die Informationssicherheit: Artikel 25 und 32 DSGVO fordern die Umsetzung dieser Maßnahmen zur Gewährleistung von Datensicherheit nach aktuellem Stand der Technik, jedoch stets im angemessenen Verhältnis zum jeweiligen Schutzzweck sowie unter Berücksichtigung datenschutzfreundlicher Voreinstellungen.

In Kooperation mit Ihrem DSK (Datenschutzkoordinator) haben wir die nachfolgenden TOM im DSMS dokumentiert.

Diagramm



Übersicht

Bezeichnung	Status	Letzte Änderung

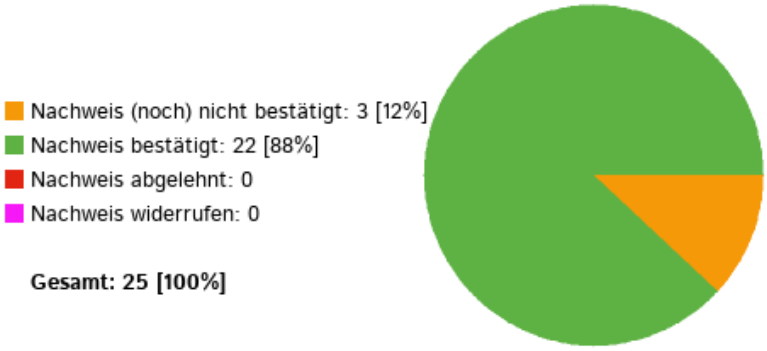
Allgemeine technische und organisatorische Maßnahmen (TOM)	Geprüft (OK)	21.04.2022

Organisatorische Maßnahmen - Mitarbeiternachweise – das O in TOM

Zur Gewährleistung eines höchstmöglichen IT-Sicherheitsniveaus sind – neben den technischen – auch organisatorische Sicherheitsmaßnahmen umzusetzen. Ein wichtiger Baustein stellt die Sensibilisierung der Mitarbeiter dar (inkl. Nachweis dessen). Zusätzlich zu der Online-Schulung sollten die im Unternehmen geltenden Regelungen in Form von Richtlinien verschriftlicht und von den Mitarbeitenden nachweislich zur Kenntnis genommen werden.

Im DSMS wurden alle der notwendigen Regelungen bereitgestellt und der DSK zur Prüfung vorgelegt vorgelegt. Den „Status quo“ der Bestätigungen zeigen das Diagramm sowie die Übersichtsliste.

Diagramm



Übersicht

Bezeichnung	Status	SOLL	IST
BetRe I Leitfaden: Datenschutzanfrage	bestätigt	2	2
DSV I Leitfaden: Datenschutzvorfall	bestätigt	2	2
MA-DS I Einverständniserklärung zur Nutzung von Foto- und / oder Filmdaten	bestätigt	2	2
MA-DS I Verpflichtungserklärung	bestätigt	2	2
TOM I Richtlinie (BYOD)	bestätigt	2	2

TOM I Richtlinie für ein sicheres Passwort	bestätigt	2	2
TOM I Richtlinie zum Umgang mit Besuchern und Firmenfremden	bestätigt	2	2
TOM I Richtlinie zum Umgang mit Internet und E-Mail	bestätigt	2	2
TOM I Richtlinie zum Umgang mit IT-Systemen am Arbeitsplatz	bestätigt	2	2
TOM I Richtlinie zum Umgang mit mobilen Arbeitsplätzen (inkl. zeitl. Beschränkung)	in Bearbeitung	2	0
TOM I Richtlinie zum Umgang mit mobilen Arbeitsplätzen (Ohne zeitl. Beschränkung)	bestätigt	2	2
TOM I Richtlinie zum Umgang mit mobilen Endgeräten	bestätigt	2	2

Betroffenen-Rechte (BetRe)

Datenschutzinformationen zu Betroffenen-Rechten

Unternehmen sind dazu verpflichtet, betroffene Personen über die Erhebung und Verarbeitung ihrer personenbezogenen Daten zu informieren. Mit dieser Informationspflicht wird der Grundsatz der Transparenz berücksichtigt. Der Zeitpunkt und Umfang der Information variieren hinsichtlich der Erhebungsart der Daten. Unterschieden wird hierbei zwischen personenbezogenen Daten, die direkt bei der betroffenen Person erhoben werden (Art. 13 DSGVO) und denen, die durch Dritte oder aus öffentlichen Quellen (Art. 14 DSGVO) erfasst werden.

Im Berichts-Zyklus wurden folgende aufgetretene Betroffenenrechte-Informationen erfasst, bearbeitet und dokumentiert; in der folgenden Übersicht bekommen Sie einen Einblick in den „Status quo“ der Dokumentation.

Erstellte Betroffenenrechte-Informationen:

Extern – in E-Mail Signatur eingebaut und nur per Link erreichbar. https://northrock.software/company-privacy
Intern – auf interner Plattform bereitgestellt und allen Beschäftigten zugänglich.

Anfragen Betroffener

Gemäß Art. 15 DSGVO haben Einzelpersonen das Recht, formlos und ohne Angabe von Gründen eine Kopie aller ihrer personenbezogenen Daten anzufordern, die durch den Verantwortlichen verarbeitet werden. Dieser sogenannten Betroffenenanfrage muss stets entsprochen werden.

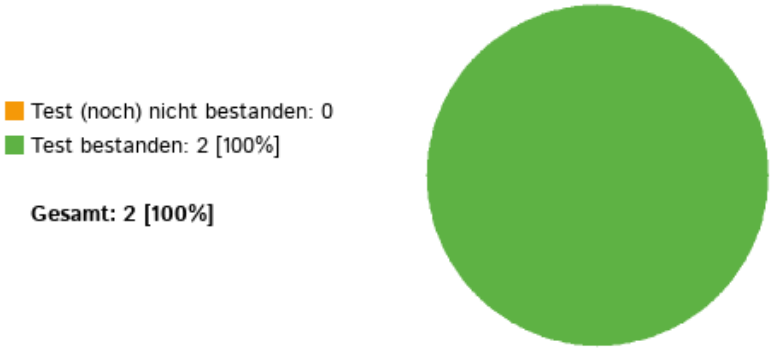
Im letzten Berichts-Zyklus sind unter unseren Kontaktdaten keine Betroffenenanfragen eingegangen respektive weitergeleitet worden. Sofern bei Ihnen besagte Anfragen eingehen, leiten Sie diese gerne an uns weiter. Die Beantwortung kann sowohl durch Sie als auch uns erfolgen; eine Dokumentation ist zwingend notwendig und sollte im DSMS vorgenommen werden.

Mitarbeiter Datenschutz (MA-DS)

DS Mitarbeiter Portal Lerntestübersicht

Beschäftigte, die regelmäßig personenbezogene Daten verarbeiten (zum Beispiel alle mit eigener E-Mail-Adresse) müssen zum datenschutzkonformen Umgang mit diesen Daten entsprechend geschult bzw. sensibilisiert werden. Zur effizienten Umsetzung dieser Vorgabe wurde für die betreffenden Mitarbeiter eine Online-Lerneinheit bereitgestellt, deren erfolgreicher Abschluss mittels eines Tests nachgewiesen wird. Alle ein bis zwei Jahre sollte eine Auffrischungs-Schulung stattfinden. Den „Status quo“ der aktuellen erfolgreichen Teilnahmen zeigen das Diagramm sowie die Übersichtsliste.

Diagramm



Übersicht

Bezeichnung	Status	SOLL	IST
Allgemeine Einführung in den Datenschutz für Beschäftigte	bestanden	2	2

Datenschutz- und Sicherheitsvorfälle (DSV)

Ein Datenschutzvorfall liegt immer dann vor, wenn der eingetretene Umstand eine potenzielle Verletzung für die Rechte und Freiheiten der betroffenen Personen nach sich ziehen kann; unabhängig davon, ob der Vorfall direkt oder indirekt durch einen Verstoß gegen das Datenschutzrecht oder trotz Umsetzung aller datenschutzrechtlich geforderten Maßnahmen eingetreten ist. Ein meldepflichtiger Vorfall muss innerhalb von 72 Stunden bei der zuständigen Behörde und ggfs. den betroffenen Personen offengelegt werden. Um diese Frist einhalten zu können, sollte bei Unklarheiten hinsichtlich einer Meldepflicht stets Rücksprache mit dem DSB gehalten werden.

Im Berichts-Zyklus wurden keine Datenschutz- und Sicherheitsvorfälle gemeldet.

Datenschutzfolgenabschätzung (DSFA)

Die Datenschutz-Grundverordnung wurde als Instrument der datenschutzrechtlichen Risikobetrachtung und -bewertung reformiert. In diesem Zusammenhang stellt die DSFA eine Verpflichtung für das verantwortliche Unternehmen dar, für bestimmte Prozesse eine ausführliche Beschreibung und Bewertung der bestehenden datenschutzrechtlichen Risiken vorzunehmen. Die DSFA ist in Art. 35 DSGVO geregelt.

Im Berichts-Zyklus wurden keine DSFA umgesetzt. Sofern im Rahmen von Risikoabschätzungen verschiedener Dienstleister und Services ein hohes Risiko für die Rechte und Freiheiten Betroffener festgestellt wird, sollten entsprechende Folgenabschätzungen durchgeführt werden.

Transfer-Impact-Assessment (Drittlandtransfer – TIA)

Seit dem Wegfall des Privacy Shields fehlt eine geeignete Rechtsgrundlage zur Datenverarbeitung in den USA. Gleichzeitig sind Unternehmen häufig auf US-Dienstleister angewiesen, da vergleichbare Anbieter aus der EU meist keine gleichwertigen Alternativen darstellen oder ein Umstieg enormen Aufwand mit sich brächte. Aus diesem Grund sind wir bestrebt, jede bestehende US-Verbindung möglichst genau zu evaluieren, mit EU-Anbietern zu vergleichen und gemeinsam das Risiko abzuwägen. Dies gilt insbesondere auch für die Auswahl neuer Dienstleister.
Folgende Maßnahmen sollten für betreffende Dienstleister umgesetzt werden:

- Abschluss der neuen EU-Standardvertragsklauseln mit allen US-Dienstleistern (siehe AV-Verzeichnis)
- Dokumentierte Abwägungen
- Transfer Impact Assessment (TIA)
- Risikoanalyse (siehe Detailansicht des VVT im DSMS)