AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

1. ALLGEMEIN

1.1. Dieser Auftragsverarbeitungsvertrag ("**AVV**") regelt die Rechte und Pflichten von Concrefy als Auftragsverarbeiter und des Kunden/Auftraggebers als Verantwortlichem im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag.

1.2. Diese AVV gilt für alle Tätigkeiten, bei denen der Auftragsverarbeiter oder beauftragte Unterauftragnehmer (Sub-Verarbeiter) personenbezogene Daten des Auftraggebers verarbeiten.

1.3. Die in dieser AVV verwendeten Begriffe sind gemäß ihrer Definition in der the EU General Data Protection Regulation (GDPR) zu verstehen.

1.4. Die Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung stehen im Einklang mit der Datenschutz-Grundverordnung (DSGVO) und der niederländischen Umsetzung der General Data Protection Regulation GDPR (Algemene Verordening Gegevensbescherming – AVG).
Soweit in dieser Vereinbarung auf die GDPR verwiesen wird, gilt dies gleichermaßen als Verweis auf die entsprechenden Bestimmungen der AVG und DSGVO.

2. INHALT DER VERARBEITUNG

2.1. Die Verarbeitung erfolgt auf der Grundlage des zwischen den Parteien geschlossenen Vertrags (Angebot/Kostenvoranschlag und Allgemeine Geschäftsbedingungen von Concrefy), wonach der Auftragsverarbeiter dem Auftraggeber bestimmte Dienstleistungen erbringt, die aus Softwareanwendungen, Webportalen und damit verbundenen Supportkomponenten wie Beratung, Tests oder Wartung bestehen (der "Vertrag"). In diesem Zusammenhang verarbeitet der Auftragsverarbeiter personenbezogene Daten von autorisierten Benutzern/Nutzern (in der Regel Mitarbeiter des Auftraggebern) sowie von anderen natürlichen Personen, die in die betrieblichen Abläufe des Auftraggebern eingebunden sind, wie z. B. Mitarbeiter von Bauunternehmen, Subunternehmern, Architekten, Lieferanten, Produktionspartnern oder anderen Dritten, die vom Auftraggeber benannt wurden oder deren Daten vom Auftragsverarbeiter als für die Datenverarbeitung Verantwortlichem hochgeladen werden, zum Zweck der Bereitstellung und Erbringung der Concrefy-Lösungen und -Dienste/Dienstleistungen.

2.2. Folgende Datenkategorien werden im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet: Name, Kontaktdaten (wie E-Mail-Adresse, Telefonnummern usw.), Vertragsdaten, Anmeldedaten (Benutzername und Passwort), Protokolldaten (Datum und Uhrzeit), ausgewähltes Betriebsgerät, Unternehmen, Zugehörigkeit und Funktion im Unternehmen, Standort, Rolle im Dienst, bevorzugte Sprache, Protokolle (Bilder), Daten bei der Anforderung von Supportleistungen (z. B. "Tickets").

2.3. Daten, die im Rahmen des Dienstes für Tests, Bauprojekte und Kundenbaustellen eingegeben werden, Messdaten, Bestandsdaten, Daten zur Materialzusammensetzung, Artikelstammdaten, Finanzdaten, Auftragsdaten, fallen nicht unter diese AVV

2.4. Der Zweck der Verarbeitung personenbezogener Daten ist die Durchführung der im Hauptvertrag als Dienstleistung, Service, Leistung oder Concrefy-Lösungen bezeichneten Arbeiten oder die, für die der Auftraggeber dem Auftragsverarbeiter nachträglich Weisungen erteilt hat.

2.5. Die Dauer der Verarbeitung richtet sich nach den Bestimmungen des Hauptvertrags, wobei sich weitere Verpflichtungen aus gesetzlichen Bestimmungen ergeben können.

3. RECHTE UND PFLICHTEN DES AUFTRAGSVERARBEITERS

3.1. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich auf der Grundlage des Hauptvertrags, dieser AVV und der dokumentierten Weisungen des Auftraggebers - auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation -, es sei denn, der Auftragsverarbeiter ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem er unterliegt, dazu verpflichtet; in diesem Fall unterrichtet der Auftragsverarbeiter den Auftraggeber vor der Verarbeitung über diese rechtlichen Anforderungen, es sei denn, das einschlägige Recht verbietet eine solche Unterrichtung aus Gründen eines erheblichen öffentlichen Interesses.

3.2. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.3. Der Auftragsverarbeiter ergreift in seinem Einflussbereich alle Maßnahmen gemäß Artikel 32 DSGVO (siehe Anhang 1 zu dieser AVV). Diese Maßnahmen hängen vom technischen Fortschritt und dem Stand der Technik ab. Geringfügige Entwicklungen werden ohne Rücksprache mit dem Auftraggeber durchgeführt.

3.4. Der Auftraggeber ermächtigt den Auftragsverarbeiter, Sub-Verarbeiter (insbesondere IT-Dienstleister) einzusetzen. Es ist darauf zu achten, dass der Sub-Verarbeiter die gleichen Verpflichtungen übernimmt, die dem Auftragsverarbeiter nach dieser Vereinbarung obliegen. Kommt der Sub-Verarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Auftraggeber für die Erfüllung der Pflichten des Sub-Verarbeiters.

3.5. Die in der Liste Sub-Verarbeiter unter https://www.concrefy.com/de/sub-verarbeiter aufgeführten Sub-Verarbeiter unterliegen insbesondere der allgemeinen Genehmigung gemäß Abschnitt 3.4..

3.6. Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten nur dann in Länder außerhalb des Europäischen Wirtschaftsraums zu übermitteln, wenn geeignete Garantien für die Einhaltung der geltenden Datenschutzvorschriften bestehen (z. B. Abschluss von Mustervertragsklauseln).

3.7. Der Auftragsverarbeiter informiert den Auftraggebern mindestens sieben (7) Tage vor der Beauftragung eines neuen Sub-Verarbeiters oder der Ersetzung eines bestehenden Sub-Verarbeiters, wobei - nach alleinigem Ermessen des Auftragsverarbeiters - (i) eine E-Mail an den Auftraggebern oder (ii) eine Veröffentlichung auf dem Kundenportal oder der Kundenplattform oder (iii) eine Veröffentlichung auf https://www.concrefy.com/de/sub-verarbeiter ausreicht, und räumt dem Auftraggeber hiermit das Recht ein, der Beauftragung eines neuen Sub-Verarbeiters oder der Ersetzung eines bestehenden Sub-Verarbeiters zu widersprechen, sofern dieser Sub-Verarbeiter nachweislich nicht dasselbe oder ein vernünftigerweise vergleichbares Schutzniveau für die Verarbeitung personenbezogener Daten gewährleistet. Der Widerspruch des Auftraggebers stellt für den Auftragsverarbeiter einen wichtigen Grund dar, den Vertrag im Sinne der Vertragsbedingungen zu kündigen. Ein Widerspruch des Auftraggebers, der die oben genannten Voraussetzungen nicht erfüllt, ist unbeachtlich.

3.8. In Anbetracht der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, um seiner Verpflichtung zur Beantwortung von Anträgen auf Ausübung der Rechte der betroffenen Person gemäß Kapitel III der DSGVO nachzukommen. Wendet sich die betroffene Person direkt an den Auftragsverarbeiter, so wird dieser sie an den Auftraggeber verweisen. Voraussetzung dafür ist, dass der Auftragsverarbeiter in der Lage ist, die betroffene Person auf der Grundlage der von der betroffenen Person bereitgestellten Informationen mit dem Auftraggeber in Verbindung zu bringen. Der Auftragsverarbeiter haftet nicht für Fälle, in denen der Auftraggeber nicht vollständig, korrekt oder rechtzeitig auf die Anfrage der betroffenen Person antwortet.

3.9. Der Auftragsverarbeiter anonymisiert oder löscht alle personenbezogenen Daten innerhalb einer Frist von einhundertachtzig (180) Tagen nach Beendigung der Erbringung der Verarbeitungsdienste vollständig, es sei denn, es besteht eine Verpflichtung zur Aufbewahrung der personenbezogenen Daten nach dem

Unionsrecht oder dem Recht der Mitgliedstaaten oder die Daten sind für die Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.

3.10. Vor der Anonymisierung oder Löschung kann der Auftraggeber gegen Zahlung angemessener Kosten die personenbezogenen Daten in einem vom Auftragsverarbeiter gewählten, gängigen elektronischen Format erhalten.

3.11. Der Auftragsverarbeiter unterstützt den Auftraggebern unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen bei der Erfüllung der Verpflichtungen aus den Artikeln 32 bis 36 GDPR).

3.12. Der Auftragsverarbeiter stellt dem Auftraggeber alle Informationen zur Verfügung, die er benötigt, um die Einhaltung der Verpflichtungen nach dieser Datenschutz-Grundverordnung nachzuweisen, und führt gemäß Abschnitt 4.5 dieser Datenschutz-Grundverordnung Audits durch und trägt zu diesen bei. Der Auftraggeber erklärt sich jedoch damit einverstanden, dass Audits gemäß Abschnitt 4.5 nach dem Ermessen des Auftragsverarbeiters unter durch die Bereitstellung einer detaillierten Dokumentation über die umgesetzten Datenschutz- und Sicherheitsmaßnahmen, einschlägige Zertifizierungen oder Berichte externer Prüfer ersetzt werden können.

3.13. Der Auftragsverarbeiter muss den Auftraggeber unverzüglich benachrichtigen, wenn er der Ansicht ist, dass eine bestimmte Anweisung des Auftraggebers gegen geltende Datenschutzvorschriften verstößt.

4. RECHTE UND PFLICHTEN DES KUNDEN/AUFTRAGGEBERS

4.1. Der Auftraggeber ist allein dafür verantwortlich, die Zulässigkeit der beauftragten Verarbeitung zu beurteilen, die Rechte der betroffenen Personen zu wahren und dem Auftragsverarbeiter die erforderlichen Meldungen zu machen. Der Auftraggeber teilt dem Auftragsverarbeiter die Kontaktstelle für alle Fragen mit, die sich aus dieser AVV ergeben oder damit zusammenhängen.

4.2. Der Auftraggeber hat alle vom Hauptvertrag abweichenden oder diesen ergänzenden Aufträge, Teilaufträge oder Weisungen schriftlich zu erteilen. In dringenden Fällen können Weisungen auch mündlich erteilt werden. Der Auftraggeber hat solche Anweisungen unverzüglich schriftlich zu bestätigen.

4.3. Stellt der Auftraggeber bei der Prüfung von Auftragsergebnissen Fehler oder Unregelmäßigkeiten fest, so hat er dies dem Auftragsverarbeiter unverzüglich mitzuteilen.

4.4. Der Auftraggeber wird besondere Kategorien personenbezogener Daten nicht ohne die schriftliche Zustimmung des Auftragsverarbeiters verarbeiten. Der Auftraggeber wird keine Daten von Personen unter 14 Jahren verarbeiten.

4.5. Vorbehaltlich des Artikels 3.12 dieser AVV hat der Auftraggeber das Recht, die Einhaltung der in dieser AVV festgelegten Verpflichtungen selbst oder durch vertraglich oder gesetzlich zur Vertraulichkeit verpflichtete Dritte, die keine Wettbewerber des Auftragsverarbeiters und seiner verbundenen Unternehmen sind, vor Ort zu überprüfen. Der Auftraggeber oder ein von ihm beauftragter Dritter hat im Rahmen dieser Kontrollen die internen Sicherheitsanforderungen des Auftragsverarbeiters (insbesondere gemäß den geltenden Sicherheits- und IT-Richtlinien) einzuhalten. Aus Gründen der Vertraulichkeit oder der Sicherheit können Vor-Ort-Kontrollen bestimmter Umgebungen und Informationen (z. B. zur Beeinträchtigung von Rechten Dritter oder zum Schutz von Geschäftsgeheimnissen) im erforderlichen Umfang eingeschränkt werden. Umgebungen, die für die Verpflichtungen aus dieser AVV nicht relevant sind, sind ausdrücklich vom Einsichtsrecht des Auftraggebers ausgeschlossen.

4.6. Die Kosten der Überprüfung trägt der Auftraggeber. Die Besichtigungen müssen ohne Störung des Geschäftsbetriebes und während der allgemeinen Geschäftszeiten durchgeführt werden. Sofern nicht dringende, vom Auftraggebern zu dokumentierende Gründe dagegen sprechen, finden Inspektionen nach angemessener Vorankündigung (mindestens 30 Arbeitstage), nach Möglichkeit bis zu einem Tag nach einem einvernehmlich festgelegten Zeitplan, der die Auswirkungen des Audits auf den Betrieb des Verarbeiters minimiert, und nicht häufiger als alle 12 Monate statt.

5. SCHLUSSBESTIMMUNGEN

5.1. Änderungen und Ergänzungen dieser AVV bedürfen der Schriftform und müssen ausdrücklich als solche gekennzeichnet sein.

5.2. Sollten einzelne Bestimmungen dieser AVV unwirksam oder undurchführbar sein oder später werden, so berührt dies die Wirksamkeit der Datenschutzvereinbarung im Übrigen nicht. Die Parteien verpflichten sich, eine solche Bestimmung durch eine gültige zu ersetzen. Das Gleiche gilt für den Fall einer Vertragslücke.

5.3. Es gilt niederländisches materielles Recht unter Ausschluss des Kollisionsrechts und des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf.

5.4. Die deutsche und die englische Sprachfassung dieses Verarbeitungsvertrages werden zu Informationszwecken zur Verfügung gestellt. Nur die niederländische Sprachfassung ist zwischen den Parteien verbindlich.

Anhang 1 -Technische und organisatorische Maßnahmen gemäß Art. 32 GDPR

Vertraulich (Art. 32 Abs. 1 lit. b GDPR)

a) Zugangskontrolle

Die folgenden implementierten Maßnahmen verhindern den unbefugten Zugang zu Datenverarbeitungsanlagen:

	implementiert.
Zutrittskontrollsystem, Kartenleser (Magnet-/Chipkarte)	✓
Türsicherung (elektrischer Türöffner, Zahlenschloss, etc.)	✓
Gesicherte Türen/Fenster	✓
Zaunanlagen	✓
Schlüsselverwaltung, Dokumentation der Schlüsselvergabe	✓
Werkschutz, Pförtner, Sicherheitsdienst	✓
Alarmanlage	✓
Besondere Schutzmaßnahmen für die Aufbewahrung von Backups und/oder anderen Datenträgern	✓
Nicht-reversible Zerstörung von Datenträgern	✓
Personal- und Berechtigungsausweise	✓
Abschließbare Bereiche	✓
Besucherordnung (z.B. Abholung am Empfang, Dokumentation der Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch zum Ausgang)	✓

b) Zugangskontrolle

Die folgenden implementierten Maßnahmen verhindern den unbefugten Zugang zu Datenverarbeitungssystemen:

	umgesetzt
Persönliche und individuelle Benutzeranmeldung beim Einloggen in das System oder Firmennetzwerk	✓
Autorisierungsverfahren für Zugriffsrechte	✓
Einschränkung der berechtigten Benutzer	✓
Einzelanmeldung	✓
Passwort-Policy (Festlegung des Passwortes AVVrameters in Bezug auf Komplexität und Aktualisierungsintervall, Passwort-Historie)	✓
Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unberechtigtem Zugriff	✓
Registrierung des Zugangs zum System	✓
Zusätzliche Systemanmeldung für bestimmte Anwendungen	✓
Automatisches Sperren von Clients nach einer bestimmten Zeit ohne Benutzeraktivität (auch passwortgeschützte Bildschirme oder automatisches Pausieren)	✓
Aktuelle Firewall	✓
Aktuelle Antiviren-Software	✓

c) Zugangskontrolle

Die folgenden Maßnahmen stellen sicher, dass Unbefugte nicht auf personenbezogene Daten zugreifen können:

	Umgesetzt
Zentrale Verwaltung und Dokumentation von Berechtigungen	✓
Abschluss von Datenverarbeitungsverträgen für die Fernwartung von Datenverarbeitungssystemen, sofern die Fernwartung die Verarbeitung von PII, d.h. die Verarbeitung personenbezogener Daten, als Teil der Dienstleistung beinhaltet.	✓
Autorisierungsprozess für Berechtigungen	✓
Berechtigungsroutinen	✓
Profile/Rollen	
Verschlüsselung von Festplatten und/oder Laptops	✓
Prozess der Aufgabentrennung	✓
Nicht umkehrbare Löschung von Datenträgern	✓
Privacy Screens für mobile Datenverarbeitungssysteme	✓
Patch-Verwaltung	✓

(d) Kontrolle der Aufgabentrennung

Die folgenden Maßnahmen stellen sicher, dass personenbezogene Daten, die für unterschiedliche Zwecke erhoben werden, getrennt verarbeitet werden.

	umgesetzt
Speicherung von Datensätzen in getrennten Datenbanken	✓
Verarbeitung auf getrennten Systemen	✓
Zugriffsberechtigungen nach funktionaler Zuständigkeit	✓
Mehrmandantenfähigkeit der IT-Systeme	✓
Nutzung von Testdaten	✓
Trennung von Entwicklungs- und Produktionsumgebung	✓
Berechtigungskonzept	✓
Netzwerk-Segmentierung	✓

Integrität (Art. 32 Abs. 1 lit. b GDPR)

(a) Offenlegungskontrolle

Es ist sicherzustellen, dass personenbezogene Daten bei der Übermittlung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können und dass überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Um dies zu gewährleisten, werden die folgenden Maßnahmen umgesetzt:

	umgesetzt.
Verschlüsselung der Speichermedien von Laptops	✓
Sichere Dateiübertragung (Collaboration, Sharepoint)	✓
Sicherer Datentransport (z.B. TLS)	✓
Elektronische Signatur	✓
Sicheres WLAN	✓
Regelung für den Umgang mit mobilen Speichermedien (z.B. Laptops, USB-Stick, Mobiltelefon)	✓
Getunnelte Datenfernverbindungen (VPN = Virtual Private Network)	✓
Klassifizierung von Daten	✓

(b) Eingabekontrolle

Durch folgende Maßnahmen wird sichergestellt, dass kontrolliert werden kann, wer zu welchem Zeitpunkt personenbezogene Daten in Datenverarbeitungssystemen verarbeitet hat:

	implementiert
Zugriffsrechte	✓
Dokumentenmanagementsystem (DMS) mit Änderungshistorie	✓
Funktionale Zuständigkeiten, organisatorisch definierte Verantwortlichkeiten	✓

Verfügbarkeit und Ausfallsicherheit (Art. 32 Abs. 1 lit. b GDPR)

Kontrolle der Verfügbarkeit und Ausfallsicherheit

Die folgenden Maßnahmen stellen sicher, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind und den Auftraggebern jederzeit zur Verfügung stehen:

	implementiert.
Etabliertes Backup-Verfahren	✓
Aufbewahrungsverfahren für Backups (z.B. feuerfester Tresor, separater Brandabschnitt).	✓
Sicherstellung der Datenspeicherung im sicheren Netzwerk	✓
Installation von Sicherheitsupdates nach Bedarf	✓
Spiegelung von Festplatten	✓
Installation einer unterbrechungsfreien Stromversorgung (USV)	✓
Geeigneter Archivraum für Papierdokumente	✓
Brand- und/oder Löschwasserschutz für den Serverraum	✓
Brand- und/oder Löschwasserschutz für die Archivräume	✓
Klimatisierter Serverraum	✓
Schutz vor Viren	✓
Firewall	✓
Redundante, lokal getrennte Datenspeicherung (Offsite Storage)	✓
Überwachung aller relevanten Server	✓
Back-up-Rechenzentrum	✓
Kritische Komponenten sind redundant ausgelegt	✓

Verfahren zur periodischen Überprüfung, Beurteilung und Bewertung (Art. 32 Abs. 1 lit. GDPR; Art. 25 Abs. 1 GDPR)

(a) Datenschutzmanagement

Die folgenden Maßnahmen sollen sicherstellen, dass eine Organisation vorhanden ist, die die grundlegenden Anforderungen der Datenschutzgesetzgebung erfüllt:

	Umgesetzt
Datenschutzpolitik (Schutz von personenbezogenen Daten)	✓
Einsetzung eines Datenschutzausschusses	✓
Verpflichtung der Mitarbeiter zur Wahrung des Datengeheimnisses	✓
Überblick über die Verarbeitungstätigkeiten (Art. 30 GDPR)	✓
Datenschutzmanagement-Softwarelösung im Einsatz	✓
Zertifizierung nach ISO 9001	✓
Standardisierter Prozess zur Bearbeitung von Auskunftsersuchen und anderen Rechten der Betroffenen	✓
Zentrale Dokumentation aller Datenschutzverfahren und -regelungen mit Zugriffsmöglichkeit für Mitarbeiter auf Basis von Berechtigungen	✓

b) Vorfallsmanagement

Die folgenden Maßnahmen sollen sicherstellen, dass im Falle von Datenschutzverletzungen Meldeprozesse eingeleitet werden:

	umgesetzt
Meldeprozess für Datenschutzverletzungen gem. 4 Nr. 12 GDPR gegenüber den Aufsichtsbehörden (Art. 33 GDPR)	✓
Meldeverfahren für Datenschutzverletzungen nach Abs. 4 Nr. 12 GDPR gegenüber den betroffenen Personen (Art. 34 GDPR)	✓
Dokumentiertes Verfahren für den Umgang mit Sicherheitsvorfällen	✓

(c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 GDPR)

Bei der Einrichtung von Standardeinstellungen sollten sowohl standardisierte Voreinstellungen von Systemen und Apps als auch Datenverarbeitungsverfahren berücksichtigt werden. Hier werden Funktionen und Rechte konkret konfiguriert, die Zulässigkeit oder Unzulässigkeit bestimmter Eingaben oder Eingabemöglichkeiten (z.B. Freitexte) unter dem Gesichtspunkt der Datenminimierung definiert und Entscheidungen über die Verfügbarkeit von Nutzerfunktionen (z.B. über den Umfang der Verarbeitung) getroffen. Auch Art und Umfang der Personenreferenzierung bzw. Anonymisierung (z.B. bei Selektions-, Export- und Auswertungsfunktionen, die standardmäßig vorgegeben und verfügbar oder frei konfigurierbar sein können) oder die Verfügbarkeit bestimmter Bearbeitungsfunktionen, Protokollierungen etc. werden festgelegt.

	implementiert
Eingabefelder in Online-Formularen nur dann als Pflichtfelder kennzeichnen, wenn sie für den weiteren Prozess unbedingt erforderlich sind.	✓
Einfache Ausübung des Widerrufsrechts durch technische Maßnahmen (E-Mail-Footer).	✓

d) Auftragskontrolle

Durch folgende Maßnahmen wird sichergestellt, dass personenbezogene Daten nur auftragsgemäß verarbeitet werden können.

	umgesetzt
Auftragsverarbeitungsvertrag mit Regelungen über Rechte und Pflichten von Auftragnehmer und Auftraggeber	✓
Benennung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern	✓
Schriftliche Datenschutzbelehrung für alle Mitarbeiter mit Zugriffsrechten	✓
Verpflichtung aller Mitarbeiter mit Datenzugriffsrechten auf das Datengeheimnis.	✓