|  |  |  |  |
| --- | --- | --- | --- |
| Daten | Nutzer | Rechte | Schutzklasse |
| Grundrissplan | Vermesser | Lesen und schreiben | 3 |
|  | Planung | leserecht |  |
| Auftragsdaten | Kunde | leserecht | 3 |
|  | Bearbeiter | Lesen und schreiben |  |
| Lager | Lagerist | Lesen und schreiben | 2 |
|  | Einkauf | leserecht |  |
|  | Planung | leserecht |  |
| Persönliche Kundendaten | Planung | leserecht | 3 |
|  | Bearbeiter | Lesen und schreiben |  |

Schritt 6

Schritt 7

**Datenschutz und Datensicherheit**

**Datenschutz**

Datenschutz beschreibt den Schutz von der missbräuchlichen Verarbeitung personenbezogener Daten sowie den Schutz des Rechts auf informationelle Selbstbestimmung.

Der Datenschutz in Deutschland wird hauptsächlich durch die zwei Gesetze Datenschutz-Grundordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG-neu) geprägt.

Für die rechtmäßige Verarbeitung personenbezogener Daten ist eine Rechtsgrundlage gemäß DSGVO oder eine Einwilligungserklärung der betroffenen Personen notwendig.

Hierzu gehören beispielsweise persönliche und private Daten. Insbesondere Kontaktdaten wie Name, Telefonnummer, Anschrift, E-Mail-Adresse oder auch das Geburtsdatum oder die IP-Adresse. Ebenfalls generell formulierte Daten gehören dazu, wie zum Beispiel bestimmte Verhältnisse und Beziehungen, welche den Kategorien der personenbezogenen Daten unterfallen.

Personen können selbst darüber entscheiden was mit ihren Daten passiert (informationelle Selbstbestimmung).

**Datensicherheit**

Bei der Datensicherheit geht es um die Frage, wie die Daten am besten gegen einen Zugriff durch Unbefugte geschützt werden können. Es fängt bei einfachen, analogen Sachen, wie z.B. Datenträgern (Laptop, Stick) an. Dabei bezieht es sich auf die Schritte, welche eingeleitet werden müssen, um diese vor Diebstahl und Zugriff unbefugter zu schützen.  
Akten mit sensiblen Daten müssen beispielsweise sofort wegeräumt werden, wenn sie nicht mehr gebraucht werden.

In Bezug auf Authentizität, Integrität, Verfügbarkeit und Vertraulichkeit sind Daten DSGVO konform abzusichern wie in der Cloud oder dem sicheren Verfahren mit Daten auf der entsprechenden Kommunikationsplattform ihres Unternehmens.

**Authentizität:**

Zuweisung von Zugriffsrechten bzw. Schreib-/Leserecht von Datenbanken  
Nicht Jeder Anwender ist berechtigt die Daten zu sehen, oder Änderungen an Daten vorzunehmen.  
Hierfür werden Accounts für die jeweiligen Nutzer angelegt, welche ein Passwort von mindestens 8 Zeichen (Zahlen, Groß- und Kleinschreibung und Zeichen) haben.  
Passwörter sind nur für die Person oder Personengruppe bestimmt. Jeder Mitarbeiter bekommt einen eigenen Login, welcher nur vom Admin ausgelesen werden kann.

So wird gewährleistet, dass in Hinsicht der Autorität nur die berechtigten Nutzer auf die Daten zugreifen können und gegebenen falls wird diese Änderung auch protokolliert.

**Integrität:**

Für einen sicheren Umgang mit Daten erfolgt eine Authentifizierung und Identifizierung von Personen, die auf bestimmte Daten mit hohem Wertzugreifen wollen, um unberechtigten Zugriffe zu verhindern. Nur bestimmte Personen haben zugriff auf Änderungs- und Schreibrechte. So können versehentliche und böswillige Änderungen von Daten verhindert werden. Digitale Signaturen und Siegel können konfiguriert werden und Daten mit Prüfnummern versehen werden, um überprüfen zu können, ob diese manipuliert worden sind.

**Verfügbarkeit:**

Um die Verfügbarkeit von Daten zu gewähren wird ein regelmäßiges Backup der Dateien aus dem Datenserver, auf einen Cloudserver und ein externes Laufwerk durchgeführt. Falls es zu einem Ausfall des ersten Datenträgers kommt, kann so unter minimalem Verlust der Daten der zweite Datenträge eingesetzt werden bzw. die Daten aus der Cloud gezogen werden, sobald die Hardware erneuert wurde.

Zudem sollten immer Ersatzhardwareteile vorhanden sein, falls ein Bauteil ausfällt.

**Vertraulichkeit**

Zugriff unberechtigter dritter auf Daten muss unterbunden werden und ein Arbeitsplatz vorhanden sein welcher verhindert das dritte über die Schulter schauen können und USB Sticks müssen grundsätzlich verschlüsselt sein.

E-Mails müssen auch eine 1 zu 1 Verschlüsslung haben und gegeben Falls eine Authentifizierung via Passwort besitzen. Das Passwort sollte auch mindestens 8 Zeichen bestehend aus Groß- und klein Buchstaben, Zahlen und Sonderzeichen besitzen.

**Für Cloud und Home Office**  
Die Clients sollen über einen verschlüsselten VPN Tunnel und eine Firewall eine Verbindung zum Ethernet herstellen können und sich mittels Login auf ihren Accounts einloggen können.  
So ist es möglich, das die Mitarbeiter von überall aus arbeiten können.  
Voraussetzung ist ein sicheres Arbeitsumfeld um die Vertraulichkeit der Daten zu garantieren.