Checkliste Datensicherheit

Unser Unternehmen ist um die stetige Aufrechterhaltung und Erhöhung der Datensicherheit bemüht, um ein dem jeweiligen Risiko angemessenes Datenschutzniveau zu gewährleisten. Zu diesem Zweck nutzen wir eine Vielzahl von Datensicherheitsmaßnahmen, um die Vertraulichkeit und Integrität der personenbezogenen Daten unserer Kunden/innen, Lieferant/innen, Interessent/innen, Mitarbeiter/innen, Bewerber/innen und sonstiger Betroffenen zu gewährleisten.

Die folgende Checkliste enthält eine Übersicht über die in unserem Unternehmen bereits umgesetzten Datensicherheitsmaßnahmen (mit „Ja“ gekennzeichnet).

Datensicherheitsmaßnahmen

Zutreffendes bitte ankreuzen

|  |  |  |
| --- | --- | --- |
|  | Ja | Nein |
| Bauliche und infrastrukturelle Sicherheit: |  |  |
| Gibt es eine Zutrittskontrolle im Betrieb (z.B. Empfang, Portier, elektronisch überwachte Zutrittsbeschränkung o.ä.)? |  |  |
| Gibt es geeignete Maßnahmen gegen Einbruchsschutz (z.B. vergitterte Fenster im Erdgeschoss, Alarmanlage, Tresorverwahrung besonders heikler Daten o.ä.)? |  |  |
| Besteht im Betrieb eine gut organisierte Schlüsselverwaltung einschließlich genauer Aufzeichnungen über Aus- und Rückgabe aller Schlüssel? |  |  |
| Personelle und organisatorische Sicherheit: |  |  |
| Existiert im Betrieb eine Datenschutzrichtlinie mit Verhaltensregeln für den grundsätzlichen Umgang mit Daten, datenschutzrechtlichen Anfragen und Datenpannen? |  |  |
| Gibt es im Betrieb eine Richtlinie für den Umgang mit mobilen Datenträgern (z.B. Mobiltelefone, USB-Sticks, CD´s etc.)? |  |  |
| Besteht im Betrieb eine Richtlinie, die den Umgang der Mitarbeiter/innen mit Internet und E-Mail festlegt? |  |  |
| Wurden die Mitarbeiter/innen zur Geheimhaltung personenbezogener Daten verpflichtet (z.B. im Dienstvertrag oder durch Zusatzvereinbarung zum Dienstvertrag)? |  |  |
| Werden die Mitarbeiter/innen regelmäßig im Bereich Datenschutz geschult (z.B. Seminare, interne Schulungen, betriebliche Infoschreiben)? |  |  |
| Werden vertrauliche Unterlagen wie z.B. Personalakten, Kundendaten etc. zugriffsgeschützt gelagert (z.B. versperrte Schränke)? |  |  |
| Gibt es im Betrieb eine – ausdrücklich festgelegte – zuständige Ansprechperson bzw. Ansprechstelle für Notfälle (z.B. akuter Virenbefall, Verlust eines Datenträgers, sonstige Datenpanne o.ä.)? |  |  |
| Technische Maßnahmen (IT): |  |  |
| Sind auf allen Computern (Desktops, Laptops, Tablets) Virenschutzprogramme installiert und werden diese laufend aktualisiert? |  |  |
| Besteht ein fachkundig installiertes und laufend gewartetes Firewallsystem? |  |  |
| Wird die auf den Computern installierte Software (Betriebssystem, Programme, Webbrowser) stets auf dem aktuellen Stand gehalten? |  |  |
| Ist das betriebliche WLAN verschlüsselt und sind die WLAN-Passwörter sicher (ausreichende Länge, keine Trivialpasswörter)? |  |  |
| Gibt es für die IT-Anwendungen klar festgelegte Zugangs- und Zugriffsberechtigungen (z.B. Einräumung von Administratorrechten zur Änderung von grundlegenden Einstellungen nur für die IT-Leitung)? |  |  |
| Wurde bei Nutzung von Cloud-Diensten (Online-Speicherung) mit dem Cloud-Anbieter abgeklärt, welche Datensicherheitsstandards dieser anwendet und wo die Daten gespeichert werden? |  |  |

Die vorstehend mit „Ja“ beantworteten Maßnahmen sind in unserem Unternehmen bereits umgesetzt.

Die mit „Nein“ beantworteten Maßnahmen sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen für die Gewährleistung eines dem Risiko angemessenen Schutzniveaus in unserem Unternehmen

* nicht erforderlich; im Rahmen einer regelmäßigen Evaluierung (jährlich) wird überprüft, ob die derzeitige Risikobeurteilung noch aktuell ist.\*
* bisher als nicht erforderlich eingestuft worden, im Zuge unserer laufenden Evaluierung wird allerdings derzeit überprüft, ob und welche der Maßnahmen künftig im Unternehmen eingeführt werden sollen. Die Ergebnisse der Evaluierung werden in einer gesonderten Dokumentation und – sofern Maßnahmen erforderlich sind – einem Umsetzungsplan festgehalten werden.\*

\**Zutreffendes bitte ankreuzen*

............................................................ ............................................................ Ort, Datum Unterschrift Geschäftsinhaber/in, Geschäfts- führer/in oder Datenschutzmanager/in