ANLAGE 2
TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOM)
I.S.D. ART. 32 DSGVO

der Organisation

NoRA GmbH – Rudolf-Diesel-Strasse 32 – 49479 Ibbenbüren

Stand

13.06.2022

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1 Zutrittskontrollle	
Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Schlüssel / Schlüsselvergabe: Eine Schlüsselvergaberichtlinie liegt vor und ist dokumentiert Überwachungseinrichtung: Die Serverräume sind Videoüberwacht Das Firmengelände ist eingezäunt	Zentrale Schlüsselausgabe Besucher in Begleitung durch Mitarbeiter Sorgfalt bei der Auswahl der Reinigungsdienste
1.2 Zugangskontrolle	
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Login mit Benutzernamen und Kennwort komplexe Kennwortrichtlinie mit 30 Tage Wechselzyklus und Mindestlänge von 10 Zeichen Zwei Faktor Anmeldung bei sensiblen Anwendungen Antivirensoftware auf den Servern, Clients und mobilen Geräten Intrusion Detection Systeme Mobile Device Management Firewall Systeme Einsatz von VPN Verschlüsselung bei Remotezugriff Passwortserver auf denen Passwörter verwaltet werden und Zugriffe protokolliert werden mit zusätzlicher 2 Faktor Authentifizierung und eigenem Berechtigungssystem Web Applikation Firewall für Extern erreichbare Webabwendungen VPN Zugriffe mit zusätzlicher 2Faktor Authentifizierung	Verwalten von Benutzerberechtigungen Erstellen von Benutzerprofilen Richtlinie zur Passwortvergabe Allgemeine Richtlinie zum Datenschutz und Datensicherheit Anleitung manuelle Desktopsperre

1.3 Zugriffskontrolle	
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Aktenvernichter Externer Datenvernichter (DIN 66399 H5/S2) Protokollierung von Zugriffen auf Anwendungen (Eingabe/Änderung/ Löschen)	Berechtigungskonzept Verwaltung von Benutzerrechte durch Administratoren
1.4 Trennungskontrollen	
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Trennung von Produktiv- und Testsystem Mandantenfähigkeit in den Anwendungen Getrennte Speicherbereiche für unterschiedliche Aufgaben Getrennte Datenbanken für unterschiedliche Aufgaben	
1.5 Pseudonymisierung	
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese Zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Im Falle einer Pseudonymisierung werden die Daten getrennt von der Zuordnungsdatei verschlüsselt gespeichert	

2. **Integrität gem. Art. 32 Abs. 1 lit. DSGVO**

2.1 Weitergabekontrolle	
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Möglichkeit zur SSL Verschlüsselten Datenübertragung für Kunden und Mitarbeiter Einsatz von VPN Bereitstellungen über verschlüsselte Kanäle wie Https Daten in der Fernwartung Teamviewer werden verschlüsselt übertragen Protokollierung von Teamviewersitzungen und VPN einwahlen	Dokumentation jeder Übertragung und Fernwartung
2.2 Eingabekontrolle	
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Protokollierung der Eingabe (erfassen/ ändern/löschen) in Anwendungen Protokollierung von Fernwartungssitzungen Manuelle Erfassung von Tätigkeiten in einem CRM oder Helpdesk - System	Nachvollziehbarkeit von Eingaben anhand individueller Benutzernamen Vergabe von Rechten für die Änderung und Löschung von Daten

3. **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**

3.1 Verfügbarkeitskontrolle	
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Feuerlöscheinrichtungen im/am Serverraum Serveräume sind klimatisiert USV Systeme sind ausreichend vorhanden Raidsysteme für Festplattenspeicher sind eingerichtet Videoüberwachung für Serverräume Einsatz von Schutzprogrammen (Virenscannern / Firewalls) Datensicherungssysteme	Backup- und Recoverykonzept Kontrolle der Sicherungsvorgänge Regelmäßige Tests zur Datenwiederherstellung Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Gebäudes getrennte Partitionen für Betriebssysteme und Daten

4. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)**

4.1 Datenschutzmanagement	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Einsatz von Software für Datenschutzmanagement Zentrale Dokumentation aller Verfahrensanweisungen und Regelungen zum Datenschutz Eine Überprüfung der Wirksamkeit der technischen Maßnahmen wird mind. jährlich durchgeführt	Ein Datenschutzbeauftragter ist schriftlich bestellt worden Mitarbeiter sind geschult auf Vertraulichkeit Mitarbeiter sind auf das Datengeheimnis verpflichtet Regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz
4.2 Incident-Response-Management	
Unterstützung bei der Reaktion auf Sicherheitsverletzungen	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Einsatz von Firewalls und regelmäßige Aktualisierung Einsatz von Spamfiltern und regelmäßige Aktualisierung Einsatz von Virenscannern und regelmäßige Aktualisierung Intrusion Prevention System (IPS)	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen Einbindung des Datenschutzbeauftragen bei Sicherheitsvorfällen und Datenpannen Dokumentation von Sicherheitsvorfällen
4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)	
Privacy by design / Privacy by default	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Es werden nicht mehr personenbezogene Daten erhoben, als für den Prozess erforderlich Datenherkunft und Zulässigkeit werden geprüft Einfache Ausübung des Widerrufsrechts des Betroffenen	
4.2 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)	
Privacy by design / Privacy by default	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Es werden nicht mehr personenbezogene Daten erhoben, als für den Prozess erforderlich Datenherkunft und Zulässigkeit werden geprüft Einfache Ausübung des Widerrufsrechts des Betroffenen	

4.4 Auftragskontrolle	
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln	
Technische Maßnahmen	**Organisatorische Maßnahmen**
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (besonders unter Datenschutz und Datensicherheits Aspekten) Abschluß nowendiger Vereinbarungen zur Auftragsdatenverarbeitung und EU Standardvertragsklauseln Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer Regelungen zum Einsatz weiterer Subunternehmer Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Die Angaben dieser Anlage basieren auf der Auskunft des Auftragnehmers. Der Auftragnehmer bestätigt die Richtigkeit der oben gemachten Angaben und hat zur Kenntnis genommen, dass er Änderungen unverzüglich mitteilen und nachdokumentieren muss.

Ibbenbüren, 13.06.2022

Ort, Datum

Unterschrift