Allgemeine technische, organisatorische Maßnahmen (TOM´s) innerhalb der nbw gGmbH

Innerhalb der Verantwortungsbereiche ergreift die nbw gGmbH bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten die folgenden technischen und organisatorischen Maßnahmen.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle
Kein unbefugter Zutritt Gebäuden / Räumlichkeiten der nbw (Sicherstellung z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, bzw. Pförtner, Alarmanlagen, Videoanlagen):

- Elektronische Schlösser für bestimmte Datensicherheitsbereiche (Aktenvernichtung, Versand, Digitalisierung)
- Raumschlüssel / elektronische Schlüssel werden nur an autorisierte Mitarbeiter der nbw vergeben, die Vergabe wird dokumentiert.
- Es gilt die Schlüsselordnung der nbw.
- Während und nach der Arbeitszeit bzw. in Pausenzeiten sind alle Türen verschlossen zu halten.
- In den relevanten Bereichen (Aktenvernichtung, Versand, Digitalisierung) wird ein Besucherbuch geführt, in dem sich alle Besucher entsprechend eintragen müssen.
- Besucher erhalten eine Datenschutzbelehrung, die vom Besucher schriftlich quittiert werden muss.
- Nicht direkt in dem Bereich tätige Personen, Auftraggeber oder sonstige Besucher werden während der Zeit des Besuches eng durch einen Mitarbeiter der betreffenden Bereiche begleitet.

Zugangs- Zugriffskontrolle

Keine unbefugte Systembenutzung (z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern):

- Persönliche, sichere Passwörter (bestehend aus mindestens 8 Zeichen – inkl. Groß – und Kleinschreibung + Zahl + Sonderzeichen) für jeden relevanten Arbeitsplatz.
- Eine Passwortweitergabe ist untersagt.
- Passwortänderung mindestens einmal pro Jahr zwingend erforderlich.
- automatische Sperre der Rechner nach kurzer Nichtnutzung (Aktivierung nur nach Passworteingabe möglich)
- Arbeitsplatzsperre nach 6 falschen Passworteingaben
- Räume werden beim Verlassen verschlossen.

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems (z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen):

- Differenzierte Nutzung der einzelnen Systeme, d.h. jeder Mitarbeiter erhält nur den Zugriff auf die Daten, die zur Ausführung seiner Aufgaben benötigt.
- In den Datensicherheitsbereichen (Versand, Aktenvernichtung und Digitalisierung) werden passwortgesicherte Kopierer nur zur Erfüllung der Arbeitsaufträge genutzt.
- Eine Kameranutzung ist grundsätzlich während der Arbeitszeit untersagt.
- Taschenkontrollen bei den Mitarbeitern und Beschäftigten *(nur bei dringendem Verdacht sind möglich)*

Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

Es erfolgt eine Trennung nach Funktionen (z.B. Auftragsbearbeitung, Lohnabrechnung, usw.)

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport (z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur):

- **Siehe auch Punkt Zugriffskontrolle. Jede Veränderung der Datensätze wird automatisch protokolliert.**

Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (z.B.: Protokollierung, Dokumentenmanagement):

- **Siehe auch Punkt Zugriffskontrolle.**
- **Protokollierung des Datenverarbeitungssystems erfolgt automatisch (Software von Micos)**

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust (z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne)

- **Rasche Wiederherstellbarkeit**
- **Backup-Verfahren,**
- **Spiegeln von Festplatten (RAID-Verfahren)**
- **unterbrechungsfreie Stromversorgung (USV)**
- **Virenschutz/Firewall**
- **verschlossener klimatisierter Serverraum**
- **Transport der Datensicherheitscontainer mit firmeneigenen geschlossenen Fahrzeugen**
- **Notfallkonzept für Havariefälle (z.B. Maschinenausfall oder Verkehrsunfall mit sensiblen Materialien) –***Störungsmanagement (Anweisungen für den Störungsfall) liegt vor.*

Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers (z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen):

- Die Beauftragung der **Aktenvernichtung** erfolgt in der Regel über ein Online-Auftragsformular, welches der Auftraggeber eigenhändig mit den zur Ausführung des Auftrages erforderlichen Informationen füllt und an den Auftragnehmer verschlüsselt (SSL) online übermittelt. Eine Kopie des Auftrages geht automatisiert an den Auftraggeber.
- Kundenkontaktdaten werden im Auftragsdatensystem erfasst.

- Die Arbeitsvorbereitung terminiert und bestätigt den Auftrag gegenüber dem Auftraggeber.
- Ausführung des Auftrages (mit ausführlicher Dokumentation – z.B. Angaben zum Fahrzeug, Containeranzahl, Fahrer, usw.)
- Abrechnung und Übersendung des Vernichtungsprotokolls an Auftraggeber

- Die **Scanaufträge (Digitalisierung)** erfolgen im Rahmen eines eindeutig gestalteten Angebotes / Vertrages, dessen Umfang sowie die sich für die Vertragsparteien ergebenden Rechte und Pflichten geregelt sind.
- Der Auftraggeber ist berechtigt, beim Auftragnehmer eine Vorabkontrolle vorzunehmen.
- Die verantwortliche Stelle hat keinen Spielraum bei der Verarbeitung der Daten, der ihr zum Beispiel die Möglichkeit der Auswahl und Klassifizierung der Daten lässt. Vielmehr werden alle Scanvorlagen in einem automatisierten Verfahren eingescannt.

- Die Beauftragung der **Versandaufgaben (Lettershop)** durch den Auftraggeber erfolgt in der Regel durch schriftliche Bestätigung des eindeutigen Angebotes per Mail.
- Kundenkontaktdaten werden im Auftragsdatensystem (Kologio) erfasst.
- Die Arbeitsvorbereitung terminiert und bestätigt den Auftrag gegenüber dem Auftraggeber.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

- **Es finden regelmäßige Überprüfungen der Einhaltung der DSGVO durch einen externen Datenschutzbeauftragten statt.**

Erstunterweisungen, wiederholte Unterweisungen

Alle Beschäftigte und Mitarbeiter*innen werden erstmalig bei Beschäftigungsbeginn in der nbw und danach wiederholt (i.d.R. jährlich) zu Belangen der Datensicherheit / des Datenschutzes nachweislich unterwiesen.

Stand: 24.08.2022

Gerichtsstand: Berlin