Annex 2

Technische und organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen hat Nexis die folgenden technischen und organisatorischen Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus im Sinne von Artikel 32 DSGVO umgesetzt:

1. Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
Zutrittskontrolle
• Chipkarten / Transpondersysteme • Sicherheitsschlösser • Absicherung der Gebäudeschächte • Türen mit Knauf auf Außenseite • Schlüsselregelung / Liste • Empfang / Rezeption / Pförtner • Besucherbuch / Protokoll der Besucher • Mitarbeiter- / Besucherausweise • Besucher in Begleitung durch Mitarbeiter • Sorgfalt bei Auswahl Reinigungsdienste
Zugangskontrolle
• Login mit Benutzername & Passwort • Login mit 2-Faktor-Authentifizierung • Anti-Virus-Software Server • Anti-Virus-Software Clients • Firewall • Verschlüsselung von Datenträgern • Automatische Desktopsperre • Benutzerberechtigungskonzept • Administrierte Benutzerverwaltung • Zwingende Passwortanforderungen • Clean Desk Richtlinie • Mobile Device Policy • Remote Working Policy
Zugriffskontrolle
• Automatisierte Logauswertung • Protokollierung aller Datenzugriffe

- Protokollierung der Anwendungszugriffe
- Differenzierte Berechtigungen Daten, Anwendungen, Betriebssystem
- Differenzierte Berechtigungen lesen, ändern, löschen
- Datenverschlüsselung „at rest“
- Transportverschlüsselung „in transit“
- Reduktion von Administratorzugängen
- Sorgfalt Auswahl Administratoren
- Verwaltung der Benutzerrechte durch Administratoren

Trennungskontrolle

- Automatisierte Logauswertung
- Protokollierung aller Datenzugriffe
- Protokollierung Anwendungszugriffe
- Differenzierte Berechtigungen Daten, Anwendungen, Betriebssystem
- Differenzierte Berechtigungen lesen, ändern, löschen
- Mandantentrennung logisch
- Trennung von Test- und Produktivsystemen
- Reduktion von Administratorzugängen
- Sorgfalt Auswahl Administratoren
- Verwaltung der Benutzerrechte durch Administratoren

Pseudonymisierung

- Pseudonymisierung von Kundendaten in Dateien, wenn anwendbar und technisch möglich
- Pseudonymisierung von Kundendaten in NEXIS 4 (Analysesoftware), wenn anwendbar und technisch möglich

Weitergabekontrolle

- Starke Abschottung des internen Netzes mit Hilfe eines gesicherten Tunnels (VPN-Zugang)
- Begrenzter Mitarbeiterkreis
- Mitarbeiter geschult in Informationssicherheit
- Verpflichtung der Mitarbeiter auf sorgfältigen Umgang mit Informationen und Geheimhaltung
- E-Mail-Verschlüsselung (S/MIME / PGP)
- Einsatz von VPN
- Datenverschlüsselung „at rest“
- Transportverschlüsselung „in transit“
- Dokumentation von Datenempfängern, Speicherdauer und Sicherheitsmaßnahmen
- Regelmäßige Kontrolle der Datenübermittlungen

2. Gewährleistung der Integrität und Eingabekontrolle (Art. 32 Abs. 1 lit. b DSGVO)

- Protokollierung von Nutzeraktionen bei Eingabe von Daten
- Protokollierung von Nutzeraktionen bei Änderungen von Daten
- Protokollierung von Nutzeraktionen beim Löschen von Daten
- Protokollierung aller Aktionen in NEXIS 4 bei der Verarbeitung personenbezogener Daten
- Bedarfsfallbezogene Auswertung der Protokolle
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Kennzeichnung erfasster Daten
- Dedizierter Logserver
- Übersicht über Programme mit Zugriff auf personenbezogene Daten
- Individuelle Benutzerprofile
- Vergabe von Rechten basierend auf einem Berechtigungskonzept
- Organisatorische Festlegung von Eingabezuständigkeiten
- Verpflichtung auf das Datengeheimnis bzw. zur Vertraulichkeit/Verschwiegenheit
- Berechtigungskonzept für Logzugriff

3. Gewährleistung der Belastbarkeit von Systemen (Art. 32 Abs. 1 lit. b DSGVO)

- Lastausgleich (load balancing) der Netzwerkkomponenten
- Lastausgleich (load balancing) der Dienste
- Ausweichverarbeitungsanlagen vorhanden
- Redundante USV
- Redundante Klimatisierung
- Redundante Stromversorgung
- Redundante Brandbekämpfung
- Computer Emergency Response Team (CERT)
- Regelmäßige Penetration-Tests
- Regelmäßiges Patchen aller Systeme
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
  Regelmäßiges Training der Mitarbeiter

4. Gewährleistung der Verfügbarkeit und Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten (Art. 32 Abs. 1 lit. b, c DSGVO)

- Unterbringung der Server in spezifischem Serverraum in den Geschäftsräumen der Nexis GmbH oder dem Anbieter des Rechenzentrums
- Brandmeldeanlange (BMA)
- Feuer- und Rauchmeldeanlagen
- Wasserlose Brandbekämpfung im Serverraum
- Temperatur- und Feuchtigkeitsüberwachung Serverraum
- Klimatisierung des Serverraums
- Blitz- und Überspannungsschutz

- Unterbrechungsfreie Stromversorgung (USV)
- Notstromgenerator
- Schutzsteckdosen Severraum
- RAID-System / Festplattenspiegelung
- Videoüberwachung Serverraum
- Alarmmeldung bei unberechtigtem Zutritt zum Serverraum
- Backup & Recovery-Konzept (ausformuliert)
- Regelmäßige Kontrolle von Back-Up-Maßnahmen
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Serverräumlichkeiten in unterschiedlichem Brandabschnitt
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Getrennte Partitionen für Betriebssysteme und Daten
- Vorhandener Katastrophen- bzw. Notfallplan
- Zutrittsbegrenzung zum Serverraum
- Regelmäßige Schwachstellenanalyse

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO)

- ISMS unter Berücksichtigung ausgewählter Anforderungen der ISO/IEC 27001
- Strukturiertes Risikomanagement nach ISO/IEC 27001 und BSI
- Regelmäßige interne und externe Audits im Rahmen des Aufbaus eines ISMS nach ISO/IEC 27001
- Datenschutz-Management-Software
- Interne Verfahrensverzeichnisse werden mind. jährlich aktualisiert.
- Prozess zur Meldung neuer Verarbeitungsverfahren
- Auswahl datenschutzfreundlicher Voreinstellungen
- Prozess zur Einbindung des Datenschutzbeauftragten
- Überprüfung der getroffenen Maßnahmen nach dem PDCA-Zyklus (Plan, Do, Check, Act)

  Prozess zur Reaktion auf Datenschutzverletzungen

6. Auftragskontrolle

- Vertragsgestaltung gem. DSGVO (Art. 26, 28 DSGVO)
- Zentrale Erfassung vorhandener Dienstleister

  Vertragsmanagement und regelmäßige Aktualisierung der Verträge