Datenschutzaudit: Checkliste für Datenverantwortliche

Technische und organisatorische Maßnahmen (TOM) Art. 32 DSGVO

1. Organisationskontrolle

Stellt die Umsetzung von Datenschutzmaßnahmen nach Art. 32 Abs. 1 lit. d DSGVO sicher.

	Ja	Nein
Besteht die gesetzliche Verpflichtung zur Berufung eines Datenschutzbeauftragten (DSB)?	○	○
Wurde ein Datenschutzbeauftragter berufen (unabhängig von der vorher gehenden Frage)?	○	○
Wurden die MitarbeiterInnen (schriftlich) zum Datengeheimnis verpflichtet?	○	○
Wurde eine Schulung der MitarbeiterInnen zur Thematik Datenschutz abgehalten?	○	○
Wurde ein Datenschutzkonzept erarbeitet und wird dieses umgesetzt?	○	○
Wurde eine Datenschutzfolgeabschätzung durchgeführt?	○	○
Wurde ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 (Verantwortlicher) erstellt und wird dieses fortlaufend aktuell gehalten?	○	○
Wurde ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 (Verarbeitung im Auftrag) erstellt und wird dieses fortlaufend aktuell gehalten?	○	○

2. Zutrittskontrolle

Verhindert, dass Unbefugte Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten (gem. Art. 32 Abs. 1 lit. b DSGVO).

	Ja	Nein
Ist der Zutritt zu den Gebäuden / Büroräume(n) der Organisation beschränkt?	○	○
Sind Server- / Rechnerräume nur für befugtes Personal zugänglich?	○	○
Sind Server, NAS- oder Datensicherungssysteme sicher aufgestellt (Diebstahl, Manipulation, Sabotage, Vernichtung) ?	○	○
Ist der Zutritt zu Räumen beschränkt, in denen Datenmaterial (sowohl elektronisch in Form von Daten- oder Sicherungsdatenträgern als auch in Form von (Papier)Akten) aufbewahrt wird?	○	○
Sind elektronische Zutrittskontrollsysteme installiert?	○	○

3. Zugangskontrolle

Verhindert, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können, wobei allerdings das Wort "nutzen" sich nicht auf die Legaldefinition einer Nutzung im positiven Sinne beschränkt (gem. Art. 32 Abs. 1 lit. b DSGVO).

	Ja	Nein
Sind Benutzeridentifikation bzw. -authentifizierung eingerichtet?	○	○
Werden hierfür allgemein als sicher geltende Passwörter verwendet?	○	○
Werden bei Inaktivität der BenutzerInnen (z.B. verlassen des Arbeitsplatzes) Bildschrimsperren mit Passwortschutz verwendet?	○	○
Sind Anwendungen zum Schutz vor Schadprogrammen installiert, aktiviert und liegen diese in aktueller Fassung vor?	○	○
Ist ein Firewall-System installiert, aktiviert und liegt dieses in aktueller Fassung vor?	○	○
Für Zugriffe von außen durch z. B. Wartungspersonal etc. muss durch befugtes Personal eine (elektronische) Zustimmung erfolgen?	○	○
Die zur Datensicherung eingesetzten Datenträger liegen in verschlüsselter Form vor?	○	○
Zugriffe von Telearbeitsplätzen erfolgen ausschließlich in verschlüsselter Form und es wird hierfür Hardware verwendet, die vom Verantwortlichen gestellt wird?	○	○

Alois Kratochwill – IT Dienstleistungen u. D.V.
Kieslingerstraße 9/1/4
8430 Leibnitz, Steiermark
AUSTRIA

Gesellschaftsform: EPU
Geschäftsführung: Alois Kratochwill

Hotline: +43 (0) 664 732 84 000
SMS Gate: +43 (0) 664 732 84 001
Telefon: +43 (0) 3452 823 81
Telefax: +43 (0) 3452 823 81

UID: ATU54135706
BANK: BAWAG P.S.K
IBAN: AT37 6000 0000 7563 6399
BIC: BAWAATWW

E-Mail: office@wdns.at
Internet: https://wdns.at

Sie erreichen uns:
Montag bis Donnerstag von 07:30 - 16:30 Uhr, Freitags von 07:30 bis 14:00 Uhr

4. Zugriffskontrolle

	Ja	Nein

Stellt sicher, dass die zur Benutzung von DV-Anlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind; das personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können (gem. Art. 32 Abs. 1 lit. b DSGVO).

Wurde ein Konzept für Zugriffsberechtigungen erarbeitet und wird dieses umgesetzt?	○	○
Wurde ein Konzept für unterschiedliche Zugriffsrechte erarbeitet und wird dieses umgesetzt?	○	○
Werden Verletzungen dahingehend protokolliert?	○	○
Werden Datenträger (sowohl elektronische Datenträger als auch (Papier)Akten datenschutzkonform entsorgt?	○	○
Wurden Maßnahmen gegen Vervielfältigung (Kopierschutz) und Veränderung (Bearbeitungsschutz) eingerichtet?	○	○

5. Weitergabekontrolle

	erledigt	JA	Nein

Verhindert, dass personenbezogenen Daten bei der elektronischen Übertragung, beim physikalischen Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und dass festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist (gem. Art. 32 Abs. 1 lit. b DSGVO).

Bei der elektronischen Übertragung (z.B. E-Mail) ist eine Datenverschlüsselung eingerichtet und aktiv?	○	○
Eine regelmäßige Wartung und Überprüfung der Datenverarbeitungssysteme findet statt?	○	○
Veraltetes oder nicht funktionstüchtiges Equipment wird fachkundig und datenschutzkonform entsorgt?	○	○
Protokollierungsmaßnahmen (z. B. Logfiles) bei der Weitergabe wurden getroffen und werden umgesetzt?	○	○
Der Transport von Datenträgern findet in dafür vorgesehenen und verschlossenen Behältern statt?	○	○

6. Eingabekontrolle

	erledigt	JA	Nein

Stellt sicher, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind (gem. Art. 32 Abs. 1 lit. b DSGVO).

Erhebungen, Veränderungen und Löschungen von personenbezogenen Daten werden protokolliert?	○	○
Erhebungen, Veränderungen und Löschungen von Verwaltungsakten werden protokolliert?	○	○

7. Auftragskontrolle

	erledigt	JA	Nein

Stellt sicher, dass personenbezogene Daten, die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden (gem. Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO).

Es findet eine Verarbeitung im Auftrag gem. Art. 28 DSGVO statt?	○	○
Die Weisungsbefugnisse des Auftraggebers / Auftragverarbeiters wurden sichergestellt?	○	○
Ein Konfliktmanagement bei Verstößen oder Verdachtsfällen wurde eingerichtet?	○	○
Mechanismen zur Selbstkontrolle von Seiten des Auftragnehmers sind vorhanden?	○	○

8. Verfügbarkeitskontrolle

	erledigt	JA	Nein

Stellt sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Dazu zählen unter anderen Brandschutzmaßnahmen, Überspannungsschutz, unterbrechungsfreie Stromversorgung, Klimaanlage, RAID (Festplattenspiegelung) , Backupkonzept, Virenschutzkonzept, Schutz vor Diebstahl etc. (gem. Art. 32 Abs. 1 lit. b DSGVO).

Daten werden gegen unbeabsichtigte Löschung oder Vernichtung abgesichert?	○	○
Es liegen mehrfache Sicherungskopien vor?	○	○
Die Sicherungskopien sind gegen unbeabsichtigte Löschung oder Vernichtung abgesichert wie z.B. mehrfache Kopien an verschiedenen Aufbewahrungsorten?	○	○

9. Trennungsgebot

	erledigt	JA	Nein

Stellt sicher, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können (gem. Art. 32 Abs. 1 lit. b DSGVO).

Gemeinsam erhobene personenbezogene Daten sind getrennt voneinander verarbeitbar?	○	○
Personenbezogene Daten einzelner Betroffner sind getrennt voneinander verfüg- und verarbeitbar?	○	○

Alois Kratochwill – IT Dienstleistungen u. D.V.
Kieslingerstraße 9/1/4
8430 Leibnitz, Steiermark
AUSTRIA

Gesellschaftsform: EPU
Geschäftsführung: Alois Kratochwill

Hotline: +43 (0) 664 732 84 000
SMS Gate: +43 (0) 664 732 84 001
Telefon: +43 (0) 3452 823 81
Telefax: +43 (0) 3452 823 81

UID: ATU54135706
BANK: BAWAG P.S.K
IBAN: AT37 6000 0000 7563 6399
BIC: BAWAATWW

E-Mail: office@wdns.at
Internet: https://wdns.at

Sie erreichen uns:
Montag bis Donnerstag von 07:30 - 16:30 Uhr, Freitags von 07:30 bis 14:00 Uhr