Datenschutz-Konzept

gemäß DSGVO und Datenschutz-Anpassungsgesetz 2018

Stand vom 15.04.2018

Dominik Fenzl
Verantwortlicher gemäß DSGVO
Humerstrasse 41
4063 Hörsching
datenschutz@nwkt.at
Tel.: 0664 88 182 200

DIE NETZWERKKAPITÄNE

1 Allgemeine Angaben

1.1 Datenschutzkonzept

Dieses Datenschutzkonzept beruht auf den in Art 5 Z 1 DSGVO formulierten Grundsätzen wie Zweckbindung,
Datenminimierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit und ist rechtmäßig (Art 6 DSGVO). Die von der DSVGO geforderte Einhaltung der Verordnungskonformität (Art. 5 Z 2; Art 24 Z 1), der Einhaltung der Betroffenenrechte (Art 13-20), der Meldepflicht bei Datenschutzverletzung (Art 33-34), der Nachweis- und Rechenschaftspflicht (Art 5 Z 2, Art 24 Z 1) ist gewährleistet. Ein Kontroll- und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt (Art 32 Z 1).

1.2 Sachliche und räumliche Tätigkeit

Ich verarbeite als Unternehmen personenbezogene Daten von natürlichen Personen ab dem 18 Lebensjahr (Art 8 DSGVO) ganz oder teilweise automatisiert und habe meine Niederlassung in der EU, Humerstrasse 41, 4063 Hörsching, Österreich.

1.3 Datenschutzbeauftragter (DSB)

Trifft einer der nachfolgenden Kriterien zu, ist ein externer oder interner DSB notwendig und zu bestellen:

Kriterium	JA	Nein
Verarbeitung der Daten durch eine Behörde oder eine öffentliche Stelle, mit Ausnahme der Gerichte		X
Verarbeitung der personenbezogenen Daten stellt eine Kerntätigkeit der Organisation dar und/oder erfordert eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person		X
Verarbeitung besonders schutzwürdige Kategorien personenbezogenen Daten (Art 9 Z 1 DSGVO wie zB Gesundheitsdaten, ethische Herkunft, genetische bzw. biometrische Daten, Gewerkschaftszugehörigkeit, usw.) stellt eine Kerntätigkeit der Organisation dar		X

Da für mein Unternehmen keine der obigen Kriterien zutrifft, wird kein DSB bestellt.

1.4 Verantwortlicher Stammdaten

Der Verantwortliche und für den Datenschutz Zuständige ist:

Fenzl Dominik
Humerstrasse 41
4063 Hörsching
office@nwkt.at
Tel.: 0664 88 18 22 00

1.5 Schulungen im Bereich Datenschutz und Datensicherheit

Ich habe an folgenden Schulungen bzw. Seminaren betreffend der DSGVO teilgenommen

Bezeichnung der Veranstaltung	Veranstalter	Datum	Nachweis/Zertifikat Anhang Nr.
div. Vorträge zum Thema DSGVO	WKO	2017 & 2018	

1.6 Weiterbildung und Stand der Technik

Betreffs Weiterbildung und Stand der Technik setze ich folgende Aktivität

Aktivitäten	Veranstalter	Sonstiges
Info u. Weiterbildungsveranstaltungen	WKO Oberösterreich	regelmäßig
Social Media	All Facebook & diverse Veranstaltungen Kurse	regelmäßig
Webseiten und Co	diverse Veranstaltungen	regelmäßig

2 Datenverarbeitung / Datenverarbeitungszwecke
2.1 Zwecke und Beschreibung der Datenverarbeitung
2.1.1 Rechnungswesen und Geschäftsabwicklung

Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten, sowie an der Geschäftsabwicklung mitwirkende Dritte und Geschäftspartner inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten.

2.1.2 Kundenbetreuung und Marketing

Serviceorientierte Information und Betreuung von kategorisierten Kunden, Lieferanten und an der Geschäftsabwicklung mitwirkende Dritte bzw. Geschäftspartner inkl. deren jeweiligen Kontaktpersonen und Interessenten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) sowie Übermittlung von Newsletter und Werbematerial. Verarbeitung und Übermittlung von eigenen oder zugekauften Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot.

2.1.3 Personalverwaltung

Ich habe zur Zeit der Erstellung dieses Datenschutz-Konzeptes keine Mitarbeiter.

2.2 Wurde eine Datenschutzfolgenabschätzung durchgeführt?

JA	NEIN
	X

Wenn Ja, wann?

Wenn Nein, aus welchem Grund nicht?

Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, da. sowohl aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht – siehe Risikobewertung und Maßnahmen - ,da keine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt und da keine umfangreichen

Verarbeitungsensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt. Es gibt auch keine Überwachung öffentlich zugänglicher Bereiche durch Video.

3 Verfahrensverzeichnis
3.1 Rechnungswesen und Geschäftsabwicklung
3.1.1 Verantwortlicher

Fenzl Dominik
Humerstrasse 41
4063 Hörsching
office@nwkt.at
Tel.: 0664 88 18 22 00

3.1.2 Zweck

Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten,
sowie an der Geschäftsabwicklung mitwirkende Dritte und Geschäftspartner inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten

3.1.3 Kategorien der betroffenen Personen

Lfd. Nr.	Beschreibung der Kategorien betroffener Personen
1	Kunden und Lieferanten inkl. Kontaktpersonen beim Kunden und Lieferanten
2	An der Geschäftsabwicklung mitwirkende Dritte und Geschäftspartner inkl. deren jeweiligen Kontaktpersonen

3.1.4 Rechtsgrundlagen

Art 6 Z 1 a (Einwilligung der Betroffenen), b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen) DSGVO
§ 132 BAO
§§ 190, 212 UGB
EStG, UStG
Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) StF: BGBl. II Nr. 312/2004

3.1.5 Verträge, Zustimmungserklärungen oder sonstige Unterlagen

Unterlagen zu aufrechten Geschäftsabwicklungen, Rechnungen, erledigte Geschäftsfälle, Unterlagen gemäß Beraternorm EN 16114 und Zustimmungserklärungen sowie Verträge mit Auftrags Verarbeitern sind im Archiv abgelegt.

3.1.6 Kategorien der verarbeitenden Daten

Excel Datei: NWKT_DSGVO_2018.xls → Sheet: DSGVO 3.1.6

Kategorien der verarbeiteten Daten und ob sie an welchen Empfänger übermittelt werden sind auf Grund der konkreten Prüfung gemäß Datenminimierung nach Art 5 Z 1 DSGVO für mein Unternehmen mit (X) angekreuzt.

3.1.7 Löschungs- und Aufbewahrungsfristen

Daten Lfd. Nr.	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-5; 7-22; 24-30	Aufgrund der gesetzlichen Aufbewahrungsfristen wie z B § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z 3 auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen
6 + 23	Bis zur Beendigung der Geschäftsbeziehungen

3.2 Kundenbetreuung und Marketing

3.2.1 Verantwortlicher

Fenzl Dominik
Humerstrasse 41
4063 Hörsching
office@nwkt.at
Tel.: 0664 88 18 22 00

3.2.2 Zweck

Serviceorientierte Information und Betreuung von kategorisierten Kunden, Lieferanten und an der Geschäftsabwicklung mitwirkende Dritte bzw. Geschäftspartner inkl. deren jeweiligen Kontaktpersonen und Interessenten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B Korrespondenz) sowie teil-automatisierte Übermittlung von Newsletter und Werbematerial. Verarbeitung und Übermittlung von eigenen Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot.

3.2.3 Kategorien der betroffenen Personen

Lfd. Nr.	Beschreibung der Kategorien betroffener Personen
1	Kunden; Lieferanten, an der Geschäftsabwicklung mitwirkende Dritte und Interessenten
2	Kontaktpersonen beim Kunden; beim Lieferanten, bei an der Geschäftsabwicklung mitwirkende Dritt, beim Interessenten
3	potenzielle Interessenten, deren Adressen von Adressverlagen zugekauft oder selbst ermittelt wurden:

3.2.4 Rechtsgrundlagen

- Newsletter: Art 6 Z 1 lit a (Einwilligung der Betroffenen)
- Ansonsten: Art: 6 Z 1 lit a (Einwilligung der Betroffenen), b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen)

- § 151 GewO 1994, SA022 Kundenbetreuung und Marketing für eigene Zwecke" siehe Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) StF: BGBl. II Nr. 312/2004

3.2.5 Verträge, Zustimmungserklärungen oder sonstige Unterlagen

Zustimmungserklärungen bzw. Verträge sowie Verträge mit Auftrags Verarbeitern usw. sind im Archiv abgelegt.

3.2.6 Kategorien der verarbeitenden Daten

Excel Datei: NWKT_DSGVO_2018.xls → Sheet: DSGVO 3.2.6

Kategorien der verarbeiteten Daten und ob sie an welchen Empfänger übermittelt werden sind auf Grund der konkreten Prüfung gemäß Datenminimierung nach Art 5 Z 1 DSGVO für mein Unternehmen mit (X) an- gekreuzt.

3.2.7 Löschungs- und Aufbewahrungsfristen

Daten Lfd. Nr.	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-31	Aufgrund der gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen
32-38	Die Daten werden nach Ablauf des dritten Jahres nach dem letzten Kontakt-(Versuch) gelöscht.
Newsletter	Recht auf Widerspruch (Art 21 DSGVO)

4 Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

5.1 Handy

Bei Apps ist es schwer festzustellen, worauf sie überall Zugriff nehmen, daher verwende ich, wenn überhaupt, nur Apps, die ich vorab kontrolliert habe. Ich verwende für Firmen Interna ausschließlich Threema.

Mein Handy ist durch PIN & Face ID geschützt. Es gibt die Möglichkeit die Daten „fern zu löschen" (Security App). Ich verwende „sichere Ordner" und lösche den SMS, WLAN- sowie Telefonverlauf, mindestens 1x wöchentlich. In öffentliche WLAN-Netze wähle ich mich nicht ein und es gibt auch keine automatische Verbindung mit bekannten WLANs. Wenn ich ein neues Handy kaufe, so lass ich mein altes Handy von meinem IT-Fachmann immer vollständig löschen

5.2 Datenspeicher

Falls Datenspeicher verwenden, so sind die Daten darauf verschlüsselt und ein Passwort ist notwendig

5.3 Vertraulichkeit

Meinen Unternehmen befindet sich in einem besonderen Vertrauensverhältnis zu den Kunden und ich gehe daher mit allen erlangten Informationen verantwortungsbewusst um und wahre die Verschwiegenheit.

5.4 Integrität

a) **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, elektronische Signatur;
b) **Eingabekontrolle**: Personenbezogene Daten in das Datenverarbeitungssysteme werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt, Dokumentenmanagement

5.5 Verfügbarkeit und Belastbarkeit

a) **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum
b) Rasche **Wiederherstellbarkeit**; Backup-Strategie
c) **Löschungsfristen** für pb Daten

5.6 Pseudo-, Anonymisierung und Verschlüsselung

a) **Pseudonymisierung:** Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.
b) **Anonymisierung:** wo möglich und sinnvoll ist bzw. vor Löschung für interne Statistik
c) **Verschlüsselung:**
   Verschlüsselung von Datenträgern/Geräten
   - Sicherheit der verwendeten Technologie (Wirksamkeit)
   - Durchgängige Umsetzung Laptop, Handy, …

5.7 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Risikoanalyse
b) Datenschutzfreundliche Voreinstellungen
c) Ein Kontroll- und Verbesserungsprozess wir mindestens 1x jährlich durchgeführt
d) Weiterbildung siehe Schulung
e) Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (z.B. DATB, Vorabüberzeugungspflicht, Nachkontrollen

6 Betroffenenrechte wahren

Grundsätzlich stelle ich jedem Nutzer bzw. Betroffenen die jeweils aktuelle Version dieses Datenschutzkonzeptes auf meiner Homepage unter Datenschutz (siehe http://www.nwkt.at/datenschutzerklaerung/) zum Downloaden zur Verfügung.

Gemäß der DSGVO hat jeder Betroffene folgende Rechte:

- Recht auf Auskunft (Art 15 DSGVO)
- Recht auf Berichtigung (Art 16 DSGVO)
- Recht auf Löschung (Art 17 DSGVO)
- Recht auf Einschränkung (Art 18 DSGVO)
- Recht auf Übertragbarkeit (Art 20 DSGVO)
- Recht auf Widerspruch (Art 21 DSGVO)
- Recht auf Beschwerde bei der Datenschutzbehörde

6.1 Prozesse betreffs Betroffenenrechte

a) Ich erhalte Kenntnis, dass ein Betroffener seine Rechte geltend machen will, per Mail.
b) Sollte der Betroffene mir nicht persönlich bekannt sein, so muss ich zwecks Vermeidung einer Datenschutz-verletzung die Identität des Antragsstellers (Betroffenen) feststellen:

,Sehr geehrte Frau/Herr ...!
Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen wie z.B. pb Daten an eine falsche Person weiterzuleiten, mir eine Kopie/scann Ihres Personalausweises/Reisepasses zukommen zu lassen.
Ich danke Ihnen für Ihr Verständnis

c) Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten meinerseits mehr notwendig.
d) Identität zweifelsfrei festgestellt:=> Der Betroffene bekommt gemäß Art 19 DSGVO innerhalb von maximal 14 Tagen abhängig von seiner Anfrage in klarer und verständlicher Sprache folgende Antworten:

- Recht auf Auskunft (Art 15 DSGVO)
  Der Betroffene bekommt als Pdf
  mein aktuelles Datenschutzkonzept
  sein Stammdatenblatt mit alle pb Daten

- Recht auf Berichtigung (Art 16 DSGVO)
  Der Betroffene bekommt als Pdf
  mein aktuelles Datenschutzkonzept
  sein Stammdatenblatt mit den berichtigten pb Daten

- Recht auf Löschung (Art 17 DSGVO)
  Der Betroffene bekommt als Pdf
  mein aktuelles Datenschutzkonzept
  sein Stammdatenblatt ohne pb Daten (ausgenommen Name) als Nachweis, dass die Löschung erfolgt ist mit den Hinweis, dass
  die Daten **anonymisiert** für die interne Statistik verwendet werden
  nach Kopie des Stammdatenblattes auch das ganze Stammdatenblatt inklusive Namen unwiderruflich gelöscht wurde
  oder
  Bei einem bestehenden oder abgeschlossenem Vertrag mit dem Betroffenen werde ich Art 6 Z 1 lit f (berechtigte Interessen des Verantwortlichen) DSGVO geltend machen und kann daher auf Grund der gesetzlichen Aufbewahrungsfristen auf jeden Fall erst nach 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen die pb Daten löschen. In diesen Fällen tritt an Stelle einer Löschung der Daten eine Sperrung (Einschränkung).

- Recht auf Einschränkung (Art 18 DSGVO)
  Der Betroffene bekommt als Pdf
  mein aktuelles Datenschutzkonzept
  sein Stammdatenblatt, dem er entnehmen kann, dass bei ‚Recht auf Einschränkung geltend gemacht" ein Hackerl gesetzt ist und somit keine Verarbeitung seiner pb Daten

erfolgt.

- Recht auf Übertragbarkeit (Art 20 DSGVO)
  Der Betroffene bekommt als Pdf
  mein aktuelles Datenschutzkonzept
  sein Stammdatenblatt mit alle pb Daten
  gemäß Art 20 Z2 DSGVO übermittle ich sein Stammdatenblatt mit alle pb Daten als Cc. an einen anderen Verantwortlichen, den der Betroffene mir genannt hat.

6.1.1 Profiling light

Ich verarbeite (siehe Verfahrensverzeichnis Marketing) teil-automatisiert auch personenbezogener Daten von natürliche Personen, um Art und Form der jeweilig in Anspruch genommenen Dienstleistung/Produkt, Interessen, Ort, Branche, ..., Verhalten dieser natürlichen Person, ... zu kategorisieren und um im berechtigtes Interesse eine zielgerichtete Information und Betreuung (= simples Kundenprofil) sowie um eine personalisierte Direktwerbung (siehe E-Mail-Marketing) für meiner Kunde, Interessierten, Lieferanten, Projektpartner zu ermöglichen. Da nur eine teil-automatisiert, keine umfassende Bewertung persönlicher Aspekte natürlicher Personen, keine Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt und auch ausdrücklich damit keinerlei automatische Generierung von Einzelentscheidungen verbunden ist und es gänzlich ohne rechtliche oder ähnliche Wirkung für den Betroffenen ist, ist dies Verarbeitung daher nicht als Profiling im Sinne des DSGVO (siehe unten Referenzen), sondern als **Profiling light**, als **kundenorientierte Service** zu sehen und es bedarf darüber hinaus auch keiner Datenschutz-Folgeabschätzung.

6.1.2 E-Mail-Marketing Recht auf Widerspruch

Vorab beachte ich die sogenannte Robinson-Liste und setzte ein Hackerl bei ‚Keine Zusendungen von Werbematerial, Newsletter erwünscht" für alle natürlichen und juristischen Personen, die in dieser Liste ausdrücklich auf die Zusendung von Werbematerial sowie Werbemails verzichten, siehe https://www.rtr.at/de/tk/TKKS_ECGListe Referenz: § 7 E-Commerce-Gesetz (ECG)

Die Newsletter-Abonnenten, die ihre klare Einwilligung nach Art 4 DSGVO nachweislich abgegeben haben, werden hinreichend sowohl über Zweck, Art und Umfang der Datenverarbeitung als auch über ihre Rechte als Betroffene wie Recht auf Information, auf Auskunft und Richtigstellung, Widerspruchsrecht, auf Löschung und Einschränkung im E- Mail-Newsletter informiert. Darüberhinaus gibt es in jedem E-Mail-Newsletter die einfache und rasche Möglichkeit für den Betroffenen, sich vom E-Mail-Newsletter abzumelden (mit einem automatisierten Email, dass er von der Newsletter Liste gelöscht wurde). Sollte dieses Mail-Newsletter-Tool von einem Dritten bereitgestellt sein, so gibt es dazu eine Vereinbarung mit diesem Auftragsverarbeiter nach Art 28 DSGVO (siehe Marketing-Verzeichnis). Individuelles Tracking, auch über eine Übermittlungs- bzw. Lesebestätigung wird nicht gemacht, da dafür eine eigene Einwilligungserklärung notwendig ist. Macht ein Betroffener seine Rechte auf Widerspruch nicht mit Hilfe des Links im Newsletter geltend, sondern in einer anderen Form, sei es z.B. mündlich, schriftlich.
So gilt folgendes:

a) Sollte der Betroffene mir nicht persönlich bekannt sein, so muss ich zwecks Vermeidung einer Datenschutzverletzung die Identität des Antragsstellers (Betroffenen) feststellen:

   ‚Sehr geehrte Frau/Herr ..... !
   Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen wie z.B. pb Daten an eine falsche Person weiterzuleiten, mir eine Kopie/scann Ihres Personalausweises/Reisepasses zukommen zu lassen.
   Ich danke Ihnen für Ihr Verständnis

b) Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten meinerseits sind notwendig.

c) Identität zweifelsfrei festgestellt:
=> Der Betroffene bekommt betreffs Recht auf Widerspruch (Art 15 DSGVO) innerhalb von maximal 14 Tagen folgende Antworten:

‚Sehr geehrte Frau/Herr ..... !
Gemäß Ihrem Wunsch habe ich Sie hiermit von der Newsletter-Verteiler-Liste gelöscht. Sie erhalten keinen Newsletter oder Werbezusendungen von mir mehr."

6.2 Meldung von Datenschutzverletzungen

Die DSGVO definiert in Art 33 eine ‚Verletzung des Schutzes personenbezogener Daten" (data-breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

a) Ich erlange Kenntnis von einer Datenschutzverletzung.
b) **Innerhalb von 72 Stunden** mache ich eine Meldung mit Hilfe des ‚Muster Datenschutzverletzung" (siehe Anhang) an die gemäß Art 55 DSGVO zuständige Aufsichtsbehörde, wenn die Verletzung des Schutzes pb Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
c) Gemäß Art 34 Z3 DSGVO muss keine Benachrichtigung der Betroffenen erfolgt, da die Verletzung des Schutzes pb Daten aufgrund meiner TOMs (zB Verschlüsselung in Rest und Motion, BackUp, ...) voraussichtlich kein **hohes Risiko** für deren persönlichen Rechte und Freiheiten zur Folge hat
d) Die Datenschutzbehörde ist gegenteiliger Meinung und fordert mich auf, alle/gewisse Betroffenen zu informieren, siehe Art 34 Z4 DSGVO.
    a. Ich informiere Betroffenen umgehend mit einer entsprechenden Variation des ‚Muster Datenschutzverletzung" (siehe Anhang)
e) Ich werde alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht, siehe Art 33 Z5 DSGVO.

7 Maßnahmen

Siehe Toms

7.1 Vertraulichkeit
a) **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen mit Schlüssel
b) **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung mit Kennwörter, automatische Sperrmechanismen, Zwei Faktor – Authentifizierung;
c) **Zugriffskontrolle**: Zugriff nur durch Verantwortlichen

7.2 Integrität
d) **Eingabekontrolle**: Personenbezogene Daten in das Datenverarbeitungssystem werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt, Dokumentenmanagement

7.3 Verfügbarkeit
e) **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Virenschutz, Firewall, mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein

Ausweichrechenzentrum,

f) Rasche **Wiederherstellbarkeit**: Backup

8 Zusammenfassung

Ich sehe das hier dokumentierte Datenschutzniveau mit den gesetzten TOMs für mich als Unternehmen (siehe allgemeiner Teil) auch aufgrund meiner finanziellen, technischen und organisatorischen Beschränkungen als **angemessen und ausreichend** an.

Ich kann so gegenüber meinen Kunden mit gutem Gewissen sagen:

> *Liebe Kundin, lieber Kunde!*
> *Vertrauen zwischen mir und Ihnen ist die Grundlage und Voraussetzung für meine Beratung, daher sind auch alle Ihre persönlichen und beruflichen Daten bei mir in guten Händen. Ich sichere Ihnen zu, dass ich sorgsam und streng vertraulich damit umgehe und immer am aktuellen Stand der technischen und organisatorischen Datenschutz-Maßnahmen bin.*
> *Darauf können Sie vertrauen.*
>
> Die Netzwerkkapitäne OG

9 Anhang
9.1 Muster Datenschutzverletzung

Datenschutzverletzung

Art 33 EU-Datenschutzgrund-Verordnung (DSGVO) -
Meldung an die Aufsichtsbehörde: Österreichische Datenschutzbehörde,
Hohenstaufengasse 3, 1010 Wien
E-Mail: dsb@dsb.gv.at

1. Name und Kontaktdaten des **Verantwortlichen:**

a) **Name und Anschrift:**

b) **E-Mail-Adresse, Tel.Nr.:**

2. Name und Kontaktdaten des **externen/internen Datenschutzmanagers/-beauftragten:**

a) **Name und Anschrift:**

b) **E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie z.B. Tel. Nr.):**
datenschutz@nwkt.at

3. Beschreibung der **Art der Verletzung** des Schutzes personenbezogener Daten:

Soweit möglich, Kategorien und Anzahl der betroffenen Personen

a) soweit möglich betroffene Kategorien und ungefähre Zahl der **personenbezogenen Datensätze**:

4. Beschreibung der **wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten:

5. Beschreibung der **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung:

a) ggf. **Maßnahmen zur Abmilderung** der Auswirkungen der Verletzung:

6. Datum und Uhrzeit des Vorfalls:

Begründung, falls die Meldung länger als 72h nach dem Vorfall erfolgte:

Hörsching, am _____

_____
(Unterschrift)

9.2 Mustervertrag Auftragsdatenverarbeitung

Vereinbarung

über eine

Auftragsdatenverarbeitung nach Art 28 DSGVO

Der Verantwortliche:	Der Auftragsverarbeiter:
[*NN*] [*Anschrift*]	**Die Netzwerkkapitäne OG** Humerstrasse 41 4063 Hörsching
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben Sammlung, Speicherung, Darstellung und Verwaltung von Daten verschiedener Social Media Plattformen – Sammlung und Verwaltung verschiedener Bild und Produktdaten – Sammlung und Verwaltung verschiedener Kundendaten zur Erstellung einer Kundenwebseite – Sammlung und Verwaltung verschiedener Produktlisten und Kataloge, im Namen und auf Weisung des Auftraggebers.
Diese Vereinbarung ist als Ergänzung zu bestehenden Verträgen zwischen Auftraggeber und Auftragnehmer zu verstehen.

Folgende Datenkategorien werden verarbeitet: Benutzer-Namen, Vor- und Nachname, Benutzer-IDs verschiedener Social Media Plattformen, Autorisierungs-Token verschiedener Social Media Plattformen sowie PlugIns, Passwörter von Benutzer-Accounts, Profil-URLs, Profilbilder, Website- URLs, Telefonnummer, Email-Adressen, verschiedene Inhalte die auf Social Media Plattformen gespeichert und publiziert wurden (Zeitstempel, Post-IDs, Post-Texte, Bilder, Videos, Links, Kommentare, Bewertungen, Privatnachrichten), sonstige Anhänge und Metadaten von Social Media Inhalten, Kundendaten wie: Adressen, Mailadressen, Name und Anschrift, Kontodaten, Bilder und Produkte.

(2) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Benutzer, Mailaccounts, Bilder, Produkte, Mitarbeiter des Auftraggebers, Kunden und MA des Auftraggebers und deren MA.

2. DAUER DER VEREINBARUNG

Die Vereinbarung ist für die Dauer des zugrundenliegenden Vertrages zwischen Auftraggeber und Auftragnehmer abgeschlossen. Eine ordentliche Kündigung der Vereinbarung kann von beiden Parteien unter Einhaltung einer 3-monatigen Kündigungsfrist zu jedem Quartalsende erfolgen.

Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage/1 zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten[1]. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. PFLICHTEN DES AUFTRAGGEBERS

(1) Der Auftraggeber sichert dem Auftragnehmer zu, die von ihm bereit gestellten personenbezogenen Daten im Einklang mit den jeweils gültigen datenschutzrechtlichen Bestimmungen zu verarbeiten und zur Datenverarbeitung berechtigt zu sein.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

5. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG[2]

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

6. SUB-AUFTRAGSVERARBEITER[3]

Der Auftraggeber verpflichtet sich, den Auftragnehmer von allen Ansprüchen, welche mit oder im Zusammenhang mit den weitergegebenen Daten entstehen, Schad- und klaglos zu halten.

7. HAFTUNG

Der Auftraggeber verpflichtet sich, den Auftragnehmer von allen Ansprüchen, welche mit oder im Zusammenhang mit den weitergegebenen Daten entstehen, Schad- und klaglos zu halten.

8. SCHLUSSBESTIMMUNGEN

(1) Anwendbares Recht und Gerichtsstand

Diese Vereinbarung und alle ihre Anlagen unterliegen österreichischem Recht unter Ausschluss der Verweisungsnormen des österreichischen IPRG und der Bestimmungen des UN-Kaufrechtsabkommens.

Für alle Streitigkeiten aufgrund oder im Zusammenhang mit dieser Vereinbarung wird die ausschließliche Zuständigkeit des für den ersten Wiener Gemeindebezirk sachlich zuständigen Gerichts vereinbart.

(2) Schriftform

Änderungen und Ergänzungen dieser Vereinbarungen bedürfen der Schriftform, sofern nicht gesetzlich eine strengere Form vorgeschrieben ist. Das Erfordernis der Schriftform kann nur durch schriftliche Vereinbarung aufgehoben werden.

(3) Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam sein, so bleiben die übrigen Bestimmungen wirksam. Die Parteien verpflichten sich, im Falle der Unwirksamkeit einzelner Bestimmungen, die unwirksamen Bestimmungen durch Bestimmungen, die dem Zweck der unwirksamen Bestimmungen möglichst entsprechen, zu ersetzen.

[*Ort*], am [*Datum*]

Für den Auftraggeber:

Name, Position
Organisation

.....
[*Name samt Funktion*]

Hörsching am

Für den Auftragnehmer:

Fenzl Dominik, Geschäftsführer
Die Netzwerkkapitäne OG

.....
[*Name samt Funktion*]

9.3 Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

Sehr geehrte/r Frau/Herr

Da Sie im Rahmen Ihrer Tätigkeit möglicherweise mit personenbezogenen Daten in Kontakt kommen, verpflichte ich Sie hiermit zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit.

Ihre Verpflichtung besteht umfassend. Sie dürfen personenbezogene Daten selbst nicht ohne Befugnis verarbeiten und Sie dürfen anderen Personen diese Daten nicht unbefugt mitteilen oder zugänglich machen. Unter einer Verarbeitung versteht die EU-Datenschutz-Grundverordnung (DSGVO) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

‚Personenbezogene Daten" im Sinne der DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Aus- druck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Personsind.

Ihre Verpflichtung besteht ohne zeitliche Begrenzung und auch nach Beendigung Ihrer Tätigkeit fort.

Unter Geltung der DSGVO können Verstöße gegen Datenschutzbestimmungen nach DSG 2018 sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden. Datenschutzverstöße können zugleich eine Verletzung arbeits- oder dienstrechtlicher Pflichten bedeuten und entsprechende Konsequenzen haben. Datenschutzverstöße sind ebenfalls mit möglicherweise sehr hohen Bußgeldern für das Unternehmen bedroht, die gegebenenfalls zu Ersatzansprüchen Ihnen gegenüber führen können.

Ein unterschriebenes Exemplar dieses Schreibens reichen Sie bitte an ..... (die Personalabteilung/verantwortlichen Stelle/Verantwortliche) zurück.

.....
Ort, Datum Unterschrift Verantwortliche/verantwortlichen Stelle

Über die Verpflichtung auf das Datengeheimnis und die sich daraus ergebenden Verhaltensweisen wurde ich unterrichtet. Das Merkblatt zur Verpflichtungserklärung mit dem Abdruck der hier genannten Vorschriften habe ich erhalten.

.....

Ort, Datum Unterschrift des Verpflichteten

Art. 4 DSGVO Begriffsbestimmungen.

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

2. „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein

zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten,

die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(4) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der DBS und die Aufsichtsbehörde.