Datenschutzkonzept der Geoplex GIS GmbH

1. Einleitung

Dieses Datenschutzkonzept beruht auf den in Art 5 Z 1 DSGVO formulierten Grundsätzen wie Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität, Recht auf Vergessenwerden und Vertraulichkeit und ist rechtmäßig (Art 6 DSGVO). Die von der DSGVO 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), u.a. basierend auf der Checkliste, enthalten im letzten Kapitel dieses Datenschutzkonzeptes.

2. Sachliche und räumliche Tätigkeit

Wir verarbeiten als Kleinstunternehmen (KU) gemäß der EU-Empfehlung 2003/361/
EG personenbezogene Daten von natürlichen Personen ab dem 16. Lebensjahr (Art 8 DSGVO) ganz oder teilweise automatisiert und haben unsere Niederlassung in der EU: Geoplex GIS GmbH, Bohmter Straße 12, 49074 Osnabrück.

3. Datenschutzbeauftragter (DSB) und Verantwortlicher für den Datenschutz

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 z. B. Gesundheitsdaten, ethische Herkunft, genetische bzw. biometrische Daten, Gewerkschaftszugehörigkeit, usw.) stellt eine Kerntätigkeit der Organisation dar		X

Referenzen: Art 37 DSGVO, Erwägungsgründe 97

Da für unser Kleinstunternehmen keiner der obigen Kriterien zutrifft, wird kein DSB bestellt. Der Verantwortliche und für den Datenschutz zuständige ist:

Frederik Hilling (Geschäftsführer)
Geoplex GIS GmbH
Bohmter Straße 12
D-49074 Osnabrück

Referenzen: Art 4 Z 7 DSGVO

4. Weiterbildung und Stand der Technik

Aktivitäten	Veranstalter	sonstiges
Info- u. Weiterbildungsveranstaltungen, Homepages bzw. Newsletter	Webinare, etwa bei gruenderszene.de	regelmäßig
	https://www.datenschutz-guru.de/	Newsletter
	https://www.datenschutz-praxis.de/	Homepage
	Angebote der IHK Osnabrück - Emsland - Grafschaft Bentheim	Seminare

Referenzen: Art 4, 5-11 DSGVO

5. Sensibilisierung der Mitarbeitenden / Dienstleister

Geoplex sensibilisiert alle Mitarbeiter/-innen regelmäßig in Bezug auf den Umgang mit personenbezogenen Daten, um Sicherheitsmaßnahmen wirksam umsetzen und eventuelle Sicherheitsvorfälle rechtzeitig erkennen zu können.

Sobald die Ursache eines Sicherheitsvorfalls identifiziert wurde, müssen Maßnahmen zu dessen Behebung ergriffen werden. Häufig ist es notwendig, die betroffenen IT-Systeme oder Standorte zu isolieren, um die Auswirkung des Sicherheitsvorfalls einzudämmen. Die Behebung von Sicherheitsvorfällen muss ausführlich dokumentiert werden.

6. Datenverarbeitungen/Datenverarbeitungszwecke

Zwecke und Beschreibung der Datenverarbeitungen:

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 z. B. Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten
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, Serienbriefe und Infomaterial.
3. **Betrieb von Internetseiten:**

1. Newsletter-Versand: Information an Interessenten und Kunden insbesondere zu den Themen Geoplex und PlexMap.
2. Webseitenanalyse auf www.geoplex.de: Analyse des anonymisierten Besucherverhaltens auf unserer Webseite zur Optimierung und Nachvollziehbarkeit der Seitenbesuche (z.B. Einstiegs- und Ausstiegsseiten, Verweildauer...).
3. PlexMap Backend: User können sich auf der Webseite einloggen, um das PlexMap Backend zu besuchen (eigene Geodaten hochladen, verarbeiten und visualisieren) sowie ihr Profil editieren (Name und eMail-Adresse).

4. Datenschutz-Folgenabschätzung durchgeführt?

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, da keine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt und da keine umfangreichen Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt. Es gibt auch keine Überwachung öffentlich zugänglicher Bereiche durch Video.

Referenzen: Art 35 Z1-3 DSGVO

8. Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

Smartphone
Maßnahmen, die geeignet sind, Unbefugten den Zugang zu personenbezogenen Daten zu verwehren.

X	Verlorene Geräte werden über den Mobilfunkanbieter umgehend gesperrt	X	Vertrauliche Daten, wie personenbezogene Daten oder Zugangsdaten werden prinzipiell nicht auf den Geräten gespeichert
X	Sicherheitsmechanismen (z. B. Eingabe einer PIN oder eines Passworts, Fingerabdruck, etc.) werden genutzt	X	Eine unumgängliche Speicherung personenbezogener Daten auf dem Gerät (inklusive Speicherkarte) erfolgt ausschließlich in verschlüsselter Form
X	Es werden nur WPA2-verschlüsselte WLAN-Netzwerke verwendet	X	Das Versenden von vertraulichen Daten darf nur über verschlüsselte Systeme erfolgen. Nicht dazu gehören Whatsapp, Facebook und Skype
X	Bluetooth ist standardmäßig deaktiviert und darf nur zur Verbindung mit firmeneigenen Geräten aktiviert werden		

Zutrittskontrolle
Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

	Alarmanlage	X	Absicherung von Gebäudeschächten
	Automatisches Zugangskontrollesystem		Chipkarten-/Transponder-Schließsystem
	Schließsystem mit Codesperre	X	Manuelles Schließsystem
	Biometrische Zugangssperren		Videoüberwachung der Zugänge (eigenes Verfahrensverzeichnis notwendig!)
	Lichtschranken/Bewegungsmelder	X	Sicherheitsschlösser
X	Schlüsselregelung (Schlüssel Ausgabe etc.)		Personenkontrolle beim Pförtner / Empfang
	Protokollierung der Besucher	X	Sorgfältige Auswahl von Reinigungspersonal

	Sorgfältige Auswahl von Wachpersonal		Tragepflicht von Berechtigungsausweisen
X	Verschlossene Türen bei Abwesenheit		Fenstersicherung (Erdgeschoss)
X	Automatische Bildschirmsperre nach 10 Minuten		

Zugangskontrolle
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

X	Zuordnung von Benutzerrechten	X	Erstellen von Benutzerprofilen
X	Passwort Vergabe		Authentifizierung mit biometrischen Verfahren
X	Authentifikation mit Benutzername/ Passwort	X	Zuordnung von Benutzerprofilen zu IT Systemen
	Gehäuse für Regelungen		Richtlinien für Passwörter/löschen/ Clean Desk
	Sperren von externen Schnittstellen (USB etc.)	X	Sicherheitsschlösser
X	Schlüssel Regelung (Schlüssel Ausgabe etc.)		Personenkontrolle beim Pförtner/ Empfang
	Protokollierung der Besucher	X	Sorgfältige Auswahl von Reinigungspersonal
	Sorgfältige Auswahl von Wachpersonal		Tragepflicht von Berechtigungsausweisen
X	Einsatz von Intrusion detection Systemen	X	Verschlüsselung von mobilen Datenträgern
	Verschlüsselung von Smartphone Inhalten		Einsatz von zentrale Smartphone Administrationssoftware (zum Beispiel zum externen löschen von Daten)
X	Einsatz von Antivirensoftware	X	Verschlüsselung von Datenträgern in Laptops/Notebooks/USB
	Einsatz einer Hardware Firewall	X	Einsatz einer Software Firewall

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.

X	Erstellung eines Berechtigungskonzept	X	Verwaltung der Rechte durch System Administratoren

X	Anzahl der Administratoren auf das „Notwendigste“ reduziert	X	Passwort Richtlinie inklusive Passwort Länge, Passwort Wechsel (das Passwort muss mindestens 15 Zeichen lang sein,, und Sonderzeichen halten und alle zwei Monate geändert werden)
X	Protokollieren von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	X	Sichere Aufbewahrung von Datenträgern (Data Safe)
X	Physische Löschung von Datenträgern vor Wiederverwendung	X	Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
X	Einsatz von Aktenvernichten beziehungsweise Dienstleistern (nach Möglichkeit mit Datenschutz Güte Siegel)	X	Protokollierung der Vernichtung
X	Verschlüsselung von Datenträgern		

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.

	Einrichtungen von Standleitungen beziehungsweise VPN Tunnel	X	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
	E-Mail Verschlüsselung beziehungsweise Nutzung von Signatur Verfahren		Erstellen eine Übersicht von regelmäßigen Abruf und Übermittlungsvorgängen (siehe Verarbeitungsverzeichnis)
X	Dokumentation der Empfänger von Daten und der Zeitspanne der geplanten Überlassung beziehungsweise vereinbarte Löschfristen (siehe Verarbeitungsverzeichnis)		Beim physischen Transport: sichere Transportbehälter/-verpackungen
X	Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen	X	Verschlüsselung der übertragenen Daten

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.

X	Protokollierung der Eingabe, Änderung und Löschung von Daten	X	Erstellung einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

X	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen	X	Aufbewahrung von Formularen, von denen Daten automatisierte Verarbeitung übernommen worden sind
X	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	X	Klare Zuständigkeiten für Löschungen

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

X	Auswahl des Auftragnehmers oder Sorgfaltsgesichtspunkten	X	Vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
X	Schriftliche Weisung an den Auftragnehmer (zum Beispiel durch Auftragsdatenverarbeitungsvertrag) siehe Anhang	X	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (im Anhang)
X	Ob Auftragnehmer Datenschutzbeauftragter bestellt hat	X	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
X	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart	X	Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
X	Vertragsstrafen bei Verstößen		

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

X	Unterbrechungsfreie Stromversorgung (USV)	X	Klimaanlage im Serverräumen
X	Geräte zu überwachen von Temperatur und Feuchtigkeit in Serverräumen	X	Schutzsteckdosenleisten
X	Feuer und Rauchmelderanlagen	X	Feuerlöschgeräte in Serverräumen
X	Alarmanlage bei unberechtigten zu dritten zu Serverräumen	X	Erstellen eines Backup- und Recoverykonzepts
X	Testen von Datenwiederherstellung		Erstellen eines Notfallplans
X	Aufbewahren von Datensicherung an einem sicheren, ausgelagerten Ort	X	Serverräume nicht unter sanitären Anlagen
X	In Hochwassergebieten: Server Räume über der Wassergrenze		

Trennungsgebot
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

X	Physikalisch getrennt Speicherung auf gesonderten Systemen oder Datenträger	X	Logische Mandantentrennung (softwareseitig)
X	Erstellung eines Berechtigungskonzepts		Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
	Versehen der Datensätze mit den Zweckattributen/Datenfeldern	X	Bei pseudonymesierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einen getrennten, abgesicherten IT System
X	Festlegung von Datenbankrechten	X	Trennung von Produktiv- und Testsystem

9. Impressum und Datenschutzerklärungen

Impressum und Datenschutzerklärungen sind jeweils DSGVO-konform auf allen betriebenen (Kunden-)Webseiten, erreichbar.

10. Betroffenenrechte wahren

Grundsätzlich stellen wir jedem Nutzer bzw. Betroffenen die jeweils aktuelle Version unseres Datenschutzkonzeptes auf unserer Homepage im Sinne von Transparenz und Vertrauen zum Download bereit https://www.geoplex.de/datenschutz/ (Punkt 6 - Datenschutzkonzept)

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

10.1. Betroffenenrechte: Prozessketten

Wir erhalten Kenntnis, dass ein Betroffener seine Rechte geltend machen will, sei es z. B. mündlich, schriftlich, oder per E-Mail

- 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 wir Sie leider noch nicht persönlich kennen lernen durften, bitten wir Sie, um keine Datenschutzverletzung zu begehen – wie z. B. personenbezogene Daten an eine falsche Person

weiterzuleiten – uns eine Kopie/Scan Ihres Personalausweises/Reisepasses zukommen zu lassen. Ihrer Bitte in Sachen Datenschutz werden wir dann umgehend nachkommen. Wir danken Ihnen für Ihr Verständnis.
Mit freundlichen Grüßen,

- Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten notwendig.
- Identität zweifelsfrei festgestellt und Anfrage ist rechtens:
  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 sein Stammdatenblatt mit allen personenbezogenen Daten (Screenshot)
- Recht auf Berichtigung (Art 16 DSGVO)
- Der Betroffene bekommt als PDF sein Stammdatenblatt mit den berichtigten personenbezogenen Daten (Screenshot)
- Recht auf Löschung (Art 17 DSGVO)
- Der Betroffene bekommt als PDF sein Stammdatenblatt ohne personenbezogene Daten (ausgenommen Name) als Nachweis, dass die Löschung erfolgt ist mit dem Hinweis, dass
  - die Daten anonymisiert für die interne Statistik verwendet werden
  - nach Kopie des Stammdatenblattes auch das ganze Stammdatenblatt inklusive Namen unwiderruflich gelöscht wurde (Screenshot)
  - oder bei einem bestehenden oder abgeschlossenem Vertrag mit dem Betroffenen werde ich alle Daten löschen (~ Marketingdaten) bis auf jene, wo wir nach Art 6 Z 1 lit f ein berechtigtes Interessen des Verantwortlichen bzw. lit c (gesetzliche Verpflichtungen z. B. nach der BAO und dem UGB; vor allem Buchhaltungsunterlagen) DSGVO geltend machen können und wir werden daher aufgrund der gesetzlichen Aufbewahrungsfristen diese Daten auf jeden Fall erst nach 7 Jahren löschen; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen die personenbezogen Daten löschen.
  - In diesen Fällen tritt an Stelle einer Löschung der Buchhaltungsdaten eine Sperrung (Einschränkung).
- Recht auf Einschränkung (Art 18 DSGVO)
- Der Betroffene bekommt als PDF sein Stammdatenblatt, dem er entnehmen kann, dass bei „Recht auf Einschränkung geltend gemacht“ ein Haken gesetzt ist und somit keine Verarbeitung seiner personenbezogenen Daten erfolgt. (Screenshot)
- Recht auf Übertragbarkeit (Art 20 DSGVO)
- Der Betroffene bekommt als PDF sein Stammdatenblatt mit allen personenbezogenen Daten (als PDF, da es maschinell lesbar sein sollte)
- gemäß Art 20 Z2 DSGVO übermittle ich sein Stammdatenblatt mit allen personenbezogenen Daten per CC an einen anderen Verantwortlichen, den der Betroffene mir genannt hat per E-Mail, aber nur über eine sichere und verschlüsselte Übertragung. Ansonsten ausgedruckt per eingeschriebenen Brief auf Kosten des Betroffenen.
- Recht auf Beschwerde bei der Datenschutzbehörde

10.2. Meldung von Datenschutzverletzungen: Prozesskette

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.

- Wir erlangen Kenntnis von einer Datenschutzverletzung.
- Innerhalb von 72 Stunden melden wir mit Hilfe des „Muster- Datenschutzverletzungsmitteilung“ an die gemäß Art 55 DSGVO zuständige Aufsichtsbehörde, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Wir informieren Betroffene umgehend mit einem Anschreiben und einer Kopie der Meldemitteilung an die Datenschutzaufsichtsbehörde.
- Wir werden 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.

11. Checkliste für den jährlichen Kontroll- und Verbesserungsprozess

Die folgende Checkliste dient als Umsetzungshilfe für die Prüfung und Dokumentation des Umsetzungszustandes der Sicherheitsmaßnahmen für kleine Einrichtungen. Die Checkliste kann ebenso als Nachweis der Bemühungen zur Umsetzung der IT-Sicherheit verwendet werden.

Nr.	Frage	Verbesserungsbedarf	OK
1.	Werden neue mitarbeitende bei der Einstellung auf bestehende Regelungen und Handlungsanweisungen zur Informationssicherheit hingewiesen?		
2.	Sind die wichtigen Schlüsselpositionen durch einen Vertreter besetzt?		
3.	Haben alle mitarbeitenden eine Verpflichtung zur Wahrung des Daten Geheimnisses unterschrieben?		
4.	Werden Back-up Datenträger in einem gesonderten Raum aufbewahrt?		
5.	Sind auf allen Clients Virenschutz Programme installiert?		
6.	Werden Betriebssysteme und Anwendungen regelmäßig aktualisiert?		
7.	Gibt es eine Checkliste für mitarbeitende zur Beendigung des Arbeitsverhältnisses?		
8.	Gibt es eine Benutzer und Rechteverwaltung für IT Systeme und Anwendungen?		

9.	Gibt es Passwort Regelungen für IT Systeme und Anwendungen und werden diese umgesetzt?		
10.	Werden alle mitarbeitenden über die Regelung zur Nutzung von Standard Software informiert?		
11.	Mit ausschließlich Software aus vertrauenswürdigen Quellen installiert?		
12.	Gibt es regelmäßige Kontrollen bezüglich der installierten Software?		
13.	Sind auf allen Clients und Server automatische Updates aktiviert?		
14.	Gibt es spezielle Handlungsanweisungen und Tools zum löschen und vernichten von Daten?		
15.	Sind die Türen und Fenster in der Regel verschlossen, wenn die mitarbeitenden nicht am Platz sind?		
16.	Sind in den Büros verschließbare Schreibtische oder schränke vorhanden?		
17.	Gibt es im Büros mit Publikumsverkehr Diebstahlsicherung für IT Systeme?		
18.	Sind am mobilen Arbeitsplatz verschließbare Schreibtische oder schränke vorhanden?		
19.	Gibt es Regelungen welche dienstlichen Unterlagen am häuslichen Arbeitsplatz bearbeitet und zwischen der Institution und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen?		
20.	Ist auf ein kleines die Bildschirmsperre aktiviert?		
21.	Ist der Zugriff von mobilen Laptops auf das LAN per VPN abgesichert?		
22.	Ist die Verschlüsselung von E-Mail Kommunikation zwischen kleinen und Server aktiviert?		
23.	Ist bei allen Mobiltelefone/Smartphones die Eingabe der Geräte PIN aktiviert?		
24.	Werden alle vertraulichen Daten nur verschlüsselt auf Mobiltelefon/ Smartphones oder Speicherkarten gespeichert?		
25.	Wird bei WLAN das Verschlüsselungsverfahren VP A2 eingesetzt?		
26.	Werden die Schlüssel für den WLAN Zugriff regelmäßig gewechselt?		

Zusammenfassung

Wir sehen das hier dokumentierte Datenschutzniveau für uns als Kleinstunternehmen auch mit Blick auf unsere finanziellen, technischen und organisatorischen Möglichkeiten als angemessen und ausreichend an.

03.02.2021, Osnabrück

Die digitale Version des Datensicherheitskonzepts ist ohne Unterschrift gültig

———————————————————————————————————

Datum, Ort Unterschrift

Hinweis: Ein Original dieses Datensicherheitskonzepts mit Unterschrift ist in unserem Archiv abgelegt.