Technische und organisatorische Maßnahmen

Jeder Verantwortliche oder Auftragsverarbeiter, der selbst oder im Auftrag personenbezogene Daten verarbeitet, hat diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Einhaltung der Vorschriften der Datenschutz-Grundverordnung und des nationalen Datenschutzrechts zu gewährleisten. Über die zu treffenden technischen und organisatorischen Maßnahmen soll nach dem Grundsatz der Verhältnismäßigkeit entschieden werden. Insofern sind nur solche Maßnahmen zu treffen, die erforderlich sind. Damit sind Maßnahmen gemeint, deren Schutzwirkung in einem angemessenen Verhältnis zum Aufwand stehen, den sie verursachen.

Nachfolgend stellt unser Unternehmen daher die bei uns umgesetzten technischen und organisatorischen Maßnahmen dar, um die Einhaltung der gesetzlichen Erfordernisse schriftlich zu dokumentieren.

A. Name und Anschrift des Verantwortlichen

Notebook12 GmbH & Co. KG

Fraunhoferring 3

85238 Petershausen

Tel.: +49 (0) 8131-27717-94

E-Mail: info@notebook12.com

Technical and Organisational Measures

Every controller or processor, which, by himself or by mandate, processes personal data, has to implement the technical and organisational measures that are required in order to ensure compliance with the provisions of the General Data Protection Regulation and national data protection provisions. All technical and organisational measures need to be considered under the principle of proportionality. In this respect, only measures need to be implemented, that are specifically necessary. Measures are considered to be specifically necessary, as soon as their protective effect is in reasonable proportion with the expenditure they imply.

Following this our enterprise thus presenting the implemented technical and organisational measures, in order to document in writing the compliance with the legal requirements.

A. The name and address of the controller

Notebook12 GmbH & Co. KG

Fraunhoferring 3

85238 Petershausen

Tel.: +49 (0) 8131-27717-94

E-Mail: info@notebook12.com

B. Angaben zu den von der Notebook12 GmbH & Co. KG umgesetzten technischen und organisatorischen Maßnahmen

1. Zugangskontrolle

Eine Umsetzung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Zugangskontrolle ist notwendig. Zugangskontrolle bedeutet die Verwehrung des Zugangs durch Unbefugte zu Verarbeitungsanlagen, mit denen die Verarbeitung von personenbezogenen Daten durchgeführt wird.

Folgende Maßnahmen wurden von uns getroffen:

- Alarmanlage
- Automatisches Zugangskontrollsystem
- Chipkarten, Transponder
- Schließsystem mit Codesperre
- Manuelles Schließsystem
- Videoüberwachung der Zugänge
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Zugangskonzept
- Abschließbare Serverschränke
- Türen mit einem Knauf an der Außenseite
- Besucher: Nur in Begleitung durch Mitarbeiter

B. Information concerning the implemented technical and organisational measures by Notebook12 GmbH & Co. KG

1. Access control

An implementation of the necessary measures to guarantee access control is mandatory. Measures for access control are those likely to prevent unauthorised individuals from accessing the data processing equipment, with which personal data is processed.

The following measures have been taken by us:

- Alarm system
- Automatic access control system
- Chip cards, transponder
- Locking system with code lock
- Manual locking system
- Video surveillance of entrances
- Light barriers / motion detectors
- Security locks
- Key control
- Logging of visitors
- Careful selection of cleaning staff
- Access concept
- Lockable server cabinets
- Doors with a knob on the outside
- Visitors: Only accompanied by employees

2. Datenträgerkontrolle Zudem ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Datenträgerkontrolle erforderlich. Unter Datenträgerkontrolle versteht man eine Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern. Hierfür wurden von uns folgende Maßnahmen getroffen: - Verschlüsselung von Datenträgern - Erstellung eines Berechtigungskonzepts - Verwaltung der Rechte durch einen Systemadministrator - Beschränkung der Anzahl der Administratoren - Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten - Sichere Aufbewahrung von Datenträgern - Physische Löschung von Datenträgern vor jeder Wiederverwendung - Ordnungsgemäße Vernichtung von Datenträgern (nach DIN 66399) - Einsatz von Aktenvernichtern - Protokollierung der Vernichtung - Sichere Datenlöschung - VPN Tunnel - Weitergabe von Daten in anonymisierter oder pseudonymisierter Form	**2. Data Carrier Control** In addition, the implementation of measures to ensure data carrier control is mandatory. Data carrier control is aimed at preventing unauthorized reading, copying, altering or deleting of data carriers. The following measures have been implemented: - Encryption of data carriers - Creation of an authorisation concept - - Management of the rights by a system administrator - Limitation of the number of administrators - Password guideline including password length and changing of passwords - Logging of access to applications, particularly in the case of input, modification and deletion of data - Secure storage of data carriers - Physical deletion of data carriers before each re-use - Proper destruction of data carriers (according to DIN 66399) - Use of document shredders - Logging of destruction - Secure deletion of data - VPN tunnels - Disclosure of data in anonymised or pseudonymised form

3. Speicherkontrolle Weiterhin ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Speicherkontrolle erforderlich. Hierunter versteht man eine Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten. Hierfür haben wir folgende Maßnahmen getroffen: - Verschlüsselung von Datenträgern - Erstellung eines Berechtigungskonzepts - Verwaltung der Rechte durch einen Systemadministrator - Beschränkung der Anzahl der Administratoren - Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten - Sichere Aufbewahrung von Datenträgern - Physische Löschung von Datenträgern vor jeder Wiederverwendung - Ordnungsgemäße Vernichtung von Datenträgern (nach DIN 66399) - Einsatz von Aktenvernichtern - Protokollierung der Vernichtung - Sichere Datenlöschung	**3. Memory Control** Furthermore, the implementation of measures to ensure memory control is mandatory. Memory control aims at preventing unauthorized input of personal data and unauthorized reading, altering or deleting of personal data, that has been saved. Therefore, the following measures have been taken: - Encryption of data carriers - Creation of an authorisation concept - Management of the rights by a system administrator - Limitation of the number of administrators - Password guideline including password length and changing of passwords - Logging of access to applications, particularly in the case of input, modification and deletion of data - Secure storage of data carriers - Physical deletion of data carriers before each re-use - Proper destruction of data carriers (according to DIN 66399) - Use of document shredders - Logging of destruction - Secure deletion of data

4. Benutzerkontrolle Ferner ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Benutzerkontrolle erforderlich. Unter Benutzerkontrolle versteht man die Verhinderung der unbefugten Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung. Hierfür wurden von uns folgende Maßnahmen getroffen: - Verschlüsselung von Datenträgern - Festlegung von Datenbankrechten - VPN - Protokollierung der Eingabe, Änderung und Löschung von Daten - Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel - Erstellen von Benutzerprofilen - Authentifikation mit Benutzername/Passwort - Regelmäßige Kontrolle von Berechtigungen - Zugriffsrechteentzug beim Ausscheiden von Personen - Zuordnung von Benutzerprofilen zu IT-Systemen - Einsatz von Anti-Viren-Software - Firewall - Mobile Device Management - Mobile Device Policy - BIOS-Passwort - Automatische Desktopsperre	**4. User Control** In addition, measures to ensure user control are obligatory. User control means ensuring that no unauthorized use of automatic data processing systems by means of data transfering devices may occur. The following measures have been taken to ensure User Control: - Encryption of data carriers - Defining database rights - VPN - Logging for input, modification and deletion of data - Password guideline including password length and changing of passwords - Creating of user profiles - Authentication with username / password - Regular checks of authorisations - Withdrawal of access rights when people are leaving - Assignment of user profiles to IT systems - - Use of anti-virus software - Firewall - Mobile Device Management - Mobile Device Policy - BIOS password - Automatic desktop lock

5. Zugriffskontrolle Ferner ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Zugriffskontrolle nötig. Unter Zugriffskontrolle ist die Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben, zu verstehen. Hierfür haben wir die folgenden Maßnahmen ergriffen: - Erstellung eines Berechtigungskonzepts - Verwaltung der Rechte durch einen Systemadministrator - Beschränkung der Anzahl der Administratoren - Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten - Regelmäßige Überprüfung von Berechtigungen - Verschlüsselung mobiler IT-Systeme - Verschlüsselung mobiler Datenträger - Einsatz einer Antivirensoftware - Sorgfältige Auswahl und Überprüfung von Dienstleistern - Differenzierung zwischen Berechtigungen - Einsatz von Benutzerrollen	**5. Access Authorisation Control** In addition, necessary measures must be implemented for an access authorisation control. Access authorisation control means ensuring that persons authorised to use a data processing system, can only access data that they have been allowed to access through their access permission. The following measures have been taken by us: - Creation of an authorisation concept - Management of the rights by a system administrator - Limitation of the number of administrators - Password guideline including password length and changing of passwords - Logging of access to applications, particularly in the case of input, modification and deletion of data - Regular checks of authorisations - Encryption of mobile IT systems - Encryption of mobile data carriers - Use of anti-virus software - Careful selection and verification of service providers - Differentiation between authorisations - Utilisation of user roles

- Zugriffsrechteentzug beim Ausscheiden von Personen - Sichere Löschung von Datenträgern - Sichere Vernichtung von Datenträgern - Trennung von Test- und Produktivsystemen - Automatische Sperrmechanismen	- Withdrawal of access rights when people are leaving - Secure deletion of data carriers - Secure destruction of data carriers - Separation of test and productive systems - Automatic locking mechanisms
6. Übertragungskontrolle Ebenfalls ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Übertragungskontrolle notwendig. Übertragungskontrolle ist die Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können, angezeigt.	**6. Transmission Control** As well, the implementation of measures relating towards transmission control need to be taken. Those are measures to ensure that it is possible to examine and establish where personal data have been transmitted to or will be transmitted to or made available by data transmission devices.
Hierfür haben wir die folgenden Maßnahmen umgesetzt:	The following measures have been taken:
- Nutzung von Verschlüsselungs-Technologien - Protokollierung der Zugriffe - Nutzung von Signaturverfahren	- Use of encryption technologies - Logging of access - Use of signature procedures
7. Eingabekontrolle Zudem ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Eingabekontrolle nötig. Diese ist die Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte	**7. Data Entry Control** Furthermore, the implementation of measures for data entry control is required. Measures to control the entry of data are those which ensure that it is possible to subsequently check and determine, whether and by whom personal data has been entered or modified in data processing systems.

Verarbeitungssysteme eingegeben oder verändert worden sind. Hierfür wurden folgende Maßnahmen ergriffen: - Protokollierung der Eingabe, Änderung und Löschung von Daten - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) - Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts - Speicherung von Protokollen der Eingaben, Änderungen und Löschungen	The following measures have been taken by us: - Logging of the entry, modification and deletion of data - Traceability of entry, modification and deletion of data by individual user names (not user groups) - Storage of forms from which data, in automated processing, was adopted - Assignment of rights for the entry, modification and deletion of data on the basis of an authorisation concept - Storage of logs of entries, changes and deletion
8. Transportkontrolle Weiter ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Transportkontrolle nötig. Unter dieser versteht man die Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit (Art. 32 Abs. 1 lit. b var. 1 DS-GVO) und Integrität (Art. 32 Abs. 1 lit. b var. 2 DS-GVO) der Daten geschützt wird. Zu diesem Zweck wurden folgende Maßnahmen ergriffen: - Verschlüsselung von E-Mail	**8. Transport Control** In addition, measures relating to the transport control need to be taken. Measures for the transport control are those that ensure that personal data stays confidential (Art. 32(1)(b) var. 1 GDPR) and integral (Art. 32(1)(b) var. 2 GDPR) during transfer or during transportation of data carriers. Therefore, the following measures have been taken by us: - Encryption of email

- Beim physischen Transport: sichere Transportbehälter - Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen	- During the physical transport: safe transport containers - During the physical transport: careful selection of the transport staff and vehicles
9. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)	**9. Recoverability (Art. 32(1)(c) GDPR)**
Zudem ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Wiederherstellbarkeit, also einer Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können, nötig.	In addition, measures have to be taken to ensure Recoverability. Recoverability means a guarantee that systems can be restored in case of failure of the systems in cases of trouble.
Hierfür haben wir folgende Maßnahmen ergriffen: - Erstellung eines Datensicherungskonzepts - Testen der Datenwiederherstellung - Erstellen eines Notfallvorsorgekonzepts - Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort - Physisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern - Regelmäßige Backups	Therefore, the following measures have been taken: - Creation of a data backup concept - Test of data recovery - Creation of an emergency preparedness concept - Storage of data backup in a safe and outsourced place - Physically separated storage on separated systems or data carriers - Regularly backups
10. Zuverlässigkeit	**10. Reliability**
Auch ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Zuverlässigkeit erforderlich. Zuverlässigkeit meint die Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.	Also, the implementation of measures to ensure reliability is mandatory. Reliability means that all functions of the system are available and occuring malfunctions are reported.

Zu diesem Ziel haben wir folgende Maßnahmen umgesetzt: - Implementierung von regelmäßigen Patches und Updates innerhalb unserer Konzepte - Geplantes regelmäßiges Auslesen von Fehlerprotokollen - Bereitstellung redundanter Systeme für Notfälle - Unabhängig von einander funktionierende IT-Systeme - Automatisierte Meldung von Fehlfunktionen - Anti-Viren-Schutz	Therefore, the following measures have been taken: - Implementing of regular patches and updates into our concepts - Planned regular checks of error logs - Keep redundant systems available for emergencies - Independently functioning IT systems - Automated reporting of malfunctions - Anti-virus protection
11. Datenintegrität (Art. 32 Abs. 1 lit. b var. 2 DS-GVO) Ferner ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Datenintegrität nötig. Datenintegrität bedeutet die Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können. Hierfür wurden von uns folgende Maßnahmen umgesetzt: - Regelmäßige Backups des gesamten Systems - Speicherung auf mehreren separaten Laufwerken - Erstellung eines Datensicherungskonzepts	**11. Data Integrity (Art. 32(1)(b) var. 2 GDPR)** Furthermore, measures need to be implemented to ensure data integrity. Data integrity means ensuring that saved personal data must not be damaged by malfunctions of the system. The following measures have been taken to ensure this: - Regular backups of the whole system - Storage on several and different devices - Creation of a data backup concept

12. Auftragskontrolle Zudem ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Auftragskontrolle nötig. Diese meint die Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Hierfür wurden folgende Maßnahmen umgesetzt: - Auswahl jedes Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich der Datensicherheit) - Überprüfung und Dokumentation der bei den Auftragsverarbeitern getroffenen Sicherheitsmaßnahmen - Schriftliche Vereinbarungen mit den Auftragsverarbeitern (Verträge) - Überprüfung der Verpflichtung der Mitarbeiter der Auftragsverarbeiter auf die Verschwiegenheit - Laufende Überprüfung aller Auftragsverarbeiter und ihrer Tätigkeiten - Vertragsstrafen bei Verstößen **13. Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit. b var. 3 DS-GVO)** Auch ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Verfügbarkeitskontrolle, also einer Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind, nötig.	**12. Processor Control** The implementation of measures for the processor control is mandatory as well. Measures for processor control are those, that ensure that personal data processed on behalf of a controller, can only be processed in accordance with the instructions of the controller. The following measures have been taken by us: - Selection of each processor in the light of care aspects (especially with regards to data security) - Verification and documentation of the security measures taken by processors - Written agreements with processors (contracts) - Review of the commitment to confidentiality of the processors employees - Ongoing audits of all processors and their activities - Contractual penalties for a violation of contract **13. Availability Control (Art. 32(1)(b) var. 3 GDPR)** Furthermore, measures for the availability control need to be taken; these are those that ensure that personal data is protected against accidental deletion or loss.

Hierfür haben wir folgende Maßnahmen ergriffen: - Unterbrechungsfreie Stromversorgung (USV) - Klimaanlagen in den Serverräumen - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen - Schutzsteckdosenleisten in Serverräumen - Feuer- und Rauchmelder - Feuerlöschgeräte in Serverräumen - Alarmmeldung bei unberechtigtem Zugang zu Serverräumen - Erstellung eines Datensicherungskonzepts - Testen der Datenwiederherstellung - Erstellen eines Notfallvorsorgekonzepts - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort - Serverräume sind nicht unter sanitären Anlagen platziert - In Hochwassergebieten: Serverräume sind über der Wassergrenze platziert - Festplattenspiegelung - RAID Systeme **14. Trennbarkeit** Schließlich ist die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung der Trennbarkeit angezeigt. Hierunter versteht sich eine Gewährleistung, dass zu unterschiedlichen Zwecken erhobene	The following measures have been taken by us: - Uninterruptible Power Supply (UPS) - Air conditioning systems in server rooms - Devices for monitoring temperature and humidity in server rooms - Protection of socket strips in server rooms - Fire and smoke detection systems - Firefighting equipment in server rooms - Alarm warning in the event of unauthorised access to the server rooms - Creation of a data backup concept - Test of data recovery - Creation of an emergency preparedness concept - Storage of data backup in a safe and outsourced place - Server rooms are not placed under sanitary equipment - In flood areas: server rooms are placed above the water edge - Disk mirroring - RAID systems **14. Separation Control** The principle of separation control must also be observed. Separation control means that data collected for different purposes can be processed separately.

personenbezogene Daten getrennt verarbeitet werden können.	
Zu diesem Zweck haben wir folgende Maßnahmen ergriffen:	The following measures have been taken by us:
- Physisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern - Erstellung eines Berechtigungskonzepts - Versehen der Datensätze mit Zweckattributen / Datenfeldern - Festlegung von Datenbankrechten - Trennung von Produktivsystem und Testsystemen - Einsatz von mandantenfähigen Systemen	- Physically separated storage on separated systems or data carriers - Creation of an authorisation concept - Definition of data records with purposeful attributes / data fields - Defining database rights - Separation between the productive system and test systems - Use of multi-client capable systems
15. Pseudonymisierung (Art. 32 Abs. 1 lit. a, 25 Abs. 1 DS-GVO) Als Pseudonymisierung ist eine Verarbeitung personenbezogener Daten anzusehen, welche ohne Hinzuziehung zusätzlicher Informationen nicht mehr gestattet, eine Information einer spezifischen betroffenen Person zuzuordnen. Im Rahmen der Pseudonymisierung werden die zusätzlichen Informationen gesondert aufbewahrt oder gespeichert und durch geeignete technische und organisatorische Maßnahmen vor unberechtigtem Zugriff bzw. der Entpseudonymisierung geschützt.	**15. Pseudonymisation (Art. 32(1)(a), 25(1) GDPR)** Pseudonymisation is processing of personal data which, without the use of additional information, no longer allows the data to be assigned to a specific data subject. In the context of pseudonymisation, the additional information is stored or saved separately and protected against unauthorized access or de-pseudonymisation by means of appropriate technical and organisational measures.
Zu diesem Zweck haben wir folgende Maßnahmen ergriffen:	The following measures have been taken by us:

- Pseudonymisierung von Daten in Testsystemen
- Pseudonymisierung von personenbezogenen Daten, die nicht mehr im Klartext benötigt werden
- Interne Richtlinie: Personenbezogene Daten sind im Falle einer Weitergabe oder nach Ablauf von Aufbewahrungsfristen zu anonymisieren oder zu pseudonymisieren

16. Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

Als Verschlüsselung bezeichnet man die Umwandlung von Klartext in einen schlüsselabhängigen Geheimtext. Nach einer Verschlüsselung kann der Klartext nur unter Verwendung des korrekten Schlüssels wiedergewonnen werden. Folglich ist der Klartext durch die Verschlüsselung vor unberechtigtem Zugriff geschützt.

Zu diesem Zweck haben wir folgende Maßnahmen ergriffen:

- Verschlüsselung von Datenträgern
- Verschlüsselung von Datenbanken
- Verschlüsselung von E-Mail
- Verschlüsselung von Webseiten (SSL)
- Verschlüsselung von Passwörtern

17. Belastbarkeit (Art. 32 Abs. 1 lit. b var. 4 DS-GVO)

Belastbarkeit bedeutet, dass Stabilität hinsichtlich der IT-Systeme gegen Ausfälle oder Angriffe – wie etwa „Denial of Service“-Angriffe – gewährleistet sein muss.

Zu diesem Zweck haben wir folgende Maßnahmen ergriffen:

- Pseudonymisation of data in test systems
- Pseudonymisation of personal data, that are no longer needed in plain text
- Internal policy: Personal data must be anonymised or pseudonymised in the event of disclosure or expiry of the retention period

16. Encryption (Art. 32(1)(a) GDPR)

Encryption is the conversion of plain text into a key-dependent ciphertext. After encryption, the plaintext can only be retrieved using the correct key. Consequently, the plaintext is protected by encryption from unauthorized access.

The following measures have been taken by us:

- Encryption of data carriers
- Encryption of databases
- Encryption of e-mail
- Encryption of websites (SSL)
- Encryption of passwords

17. Resilience (Art. 32(1)(b) var. 4 GDPR)

Resilience means stability in terms of IT systems against failures or attacks - such as "Denial of Service" attacks - must be guaranteed.

The following measures have been taken by us:

- Einsatz einer unterbrechungsfreien Stromversorgung (USV)	- Use of an uninterruptible power supply (UPS)
- Einsatz von Kühlungen in Serverräumen	- Use of cooling in server rooms
- Klimatisierte Serverräume	- Air-conditioned server rooms
- Einsatz von Load Balancing	- Use of load balancing
18. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung technischer und organisatorischer Maßnahmen (Art. 32 Abs. 1 lit. d DS-GVO)	**18. Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures (Art. 32(1)(d) GDPR)**
- Benennung eines Datenschutzbeauftragten	- Appointment of a data protection officer
- TOM Audit durch den Datenschutzbeauftragten	- TOM audit by the data protection officer
- Regelmäßige Begehungen durch den Datenschutzbeauftragten	- Regular inspections by the data protection officer
- Regelmäßige Schulungen der Beschäftigten zum Datenschutz	- Regular training of employees on data protection
- Mitarbeiterbefragungen zum Datenschutz	- Employee surveys on data protection
- Überprüfung der Technikgestaltung durch den Datenschutzbeauftragten	- Review of privacy by design by the data protection officer
- Gewährleistung von datenschutzfreundlichen Voreinstellungen durch Einbezug des Datenschutzbeauftragten	- Ensuring privacy by default settings by involving the data protection officer
- Implementierung eines Prozesses zur Durchführung von Datenschutz-Folgenabschätzungen	- Implementation of a process for the execution of data protection impact assessments
- Regelmäßige Überprüfung des Verfahrensverzeichnisses	- Regular review of the processing activity records
- Regelmäßige Überprüfung des Kategorieverzeichnisses	- Regular check of the category records

- Implementierung eines Datenschutzmanagementsystems (DSMS) / Datenschutzhandbuchs	- Implementation of a data protection management system (DPMS) / data protection handbook
Im Ergebnis ist festzuhalten, dass wir die von der Datenschutz-Grundverordnung und nationalen Datenschutzgesetzen vorgesehenen erforderlichen technischen und organisatorischen Maßnahmen bei uns im Unternehmen umgesetzt haben.	Ultimately, it is to be held in mind that we have implemented the necessary technical and organisational measures in our enterprise, as prescribed in the General Data Protection Regulation and in national data protection provisions.
Notebook12 GmbH & Co. KG Petershausen, den 01.07.2019	Notebook12 GmbH & Co. KG Petershausen, den 01.07.2019
Alexander Schmidt CEO	Alexander Schmidt CEO

Subunternehmen der Notebook12 GmbH & Co. KG

- Name: Greenmark IT GmbH

  Anschrift: Leinstraße 3, 31061 Alfeld (Leine)

  Auftragsinhalt: Hosting von Webseiten und Daten

- Name: abc-gebäudereinigung und service GmbH

  Anschrift: Dieselstrasse 9, 85757 Karlsfeld

  Auftragsinhalt: Durchführung von Reinigungsdienstleistungen

- Name: Bewachungsdienst Dipl.-Kfm. Helmut Ehrl GmbH

  Anschrift: Ringbergstraße 1, 81673 München

  Auftragsinhalt: Durchführung von Bewachungsdienstleistungen

- Name: Joachim Keuters JK IT & Networks

  Anschrift: Gartenstr. 5, 82319 Starnberg

  Auftragsinhalt: Durchführung von IT-Dienstleistungen

- Name: Trusted Network GmbH

  Anschrift: Max-Planck-Straße 1,85716 Unterschleißheim

  Auftragsinhalt: Durchführung von Rechenzentrum-Dienstleistungen

- Name: Peter Fink Gesellschaft für intelligente Entsorgung mbH

  Anschrift: Theodor-Heuss-Straße 111, 85221 Dachau

  Auftragsinhalt: Entsorgung von Papier

- Name: QT-Development GmbH

  Anschrift: Schlierachstraße 32, 83734 Hausham

  Auftragsinhalt: Durchführung von Schulungen