Die neue Datenschutz-Grundverordnung (DS-GVO)

Änderungen im Datenschutz seit dem 25.05.2018

Referent: RA Andreas Bode

Andreas Gerhard Bode
Rechtsanwaltskanzlei

CDH Bayern

10 Schritte zur Umsetzung der Datenschutz-Grundverordnung

28.06.2018, München
RA Andreas Bode
Lehrbeauftragter der Universität Hannover

Walderseestr. 14 A
30177 Hannover
http://www.vertriebundrecht.de

Tel.: 0511 66 10 23
Fax.: 0511 66 10 32
eMail: bode@vertriebundrecht.de

A n d r e a s G e r h a r d B o d e
R e c h t s a n w a l t s k a n z l e i

10 Schritte zur Umsetzung der Datenschutz-Grundverordnung

Die neue europäische Datenschutz-Grundverordnung (DS-GVO) ist am 25.05.2018 in Kraft getreten.

Es gibt keine Übergangsfrist. Soweit die DS-GVO auf Ihr Unternehmen anwendbar ist, müssen sämtliche Anforderungen der DS-GVO seit dem 25.05.2018 eingehalten werden. Andernfalls können die Datenschutzbehörden per Verwaltungsakt aufsichtsrechtliche Maßnahmen ergreifen und Bußgelder verhängen.

Deshalb ist es für Sie wichtig festzustellen, welche Anforderungen auf Ihr Unternehmen zugekommen sind. Hierzu dient die nachfolgende Checkliste zur Umsetzung der DS-GVO.

I. Kommen Sie mit personbezogenen Daten in Berührung?

Personbezogene Daten gemäß DS-GVO sind Angaben, die bei Zuordnung zu einer natürlichen Person Einblicke ermöglichen in deren physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität (zum Beispiel Personendaten, Krankenversicherungsnummer, Sozialversicherungsnummer, Bankdaten, IP-Adresse, Augenfarbe, E-Mail-Adresse …).

Haben Sie es im Unternehmen mit personenbezogenen Daten zu tun (ja/nein)?

II. Verarbeiten Sie personbezogene Daten?

Unter der Verarbeitung personenbezogener Daten ist die Erhebung, Speicherung, Änderung, Nutzung, Übermittlung, Verknüpfung oder Löschen von Daten durch den Verarbeiter zu verstehen.

Der Verarbeiter von personbezogenen Daten ist Verantwortlicher im Sinne der DS-GVO.

Nicht Gegenstand der DS-GVO ist die Datenverarbeitung für private Zwecke. Sofern Ihr Unternehmen mit personbezogenen Daten arbeitet, ist die DS-GVO anwendbar.

Verarbeiten Sie als Verantwortlicher personenbezogenen Daten im Unternehmen (ja/nein)?

Walderseestr. 14 A
30177 Hannover
http://www.vertriebundrecht.de

Tel.: 0511 66 10 23
Fax.: 0511 66 10 32
eMail: bode@vertriebundrecht.de

III. Müssen Sie ein Verarbeitungsverzeichnis erstellen?

Die DS-GVO verlangt vom Verantwortlichen die Erstellung eines Verarbeitungsverzeichnisses.

Nur wenn die Verarbeitung gelegentlich erfolgt, keine besonderen Datenkategorien, wie Gesundheits- oder Religionsdaten, verarbeitet werden und die Mitarbeiterzahl unter 250 liegt, kann ausnahmsweise von der Erstellung eines Verzeichnisses abgesehen werden.

Dies dürfte aber in der Regel nicht der Fall sein, zumal wenn Lohnabrechnungen von Mitarbeitern durchgeführt werden und Kundenkarteien angelegt werden.

Müssen Sie aufgrund der vorstehenden Ausführungen ein Verzeichnis erstellen (ja/nein)?

IV. Wie muss das Verarbeitungsverzeichnis erstellt werden?

Hierzu sind die Verarbeitungstätigkeiten im Unternehmen zu erfassen. Artikel 30 DS-GVO schreibt die Führung eines Verzeichnisses aller Verarbeitungstätigkeiten im Unternehmen vor. Das Verzeichnis dient dem Nachweis der datenschutzkonformen Datenverarbeitung im Unternehmen. Das Verarbeitungsverzeichnis ist nicht öffentlich.

Sie müssen prüfen, welche Verarbeitungstätigkeiten im Unternehmen erfolgen, zum Beispiel:

- Verarbeitung von Mitarbeiterdaten
- Aufnahme von Kundendaten
- Verarbeitung von Lieferantendaten
- Erhebung von Daten über die Website (Kontaktformular, Cookies…)
- Verarbeitung von Bewerberdaten
- Besucherdaten

Kennen Sie sämtliche Verarbeitungsvorgänge in Ihrem Unternehmen (ja/nein)?

Walderseestr. 14 A
30177 Hannover
http://www.vertriebundrecht.de

Tel.: 0511 66 10 23
Fax.: 0511 66 10 32
eMail: bode@vertriebundrecht.de

IV. Wie muss das Verarbeitungsverzeichnis aussehen?

Das Verarbeitungsverzeichnis kann wie folgt aussehen (siehe auch Muster in der Anlage):

Name und Anschrift des Verantwortlichen	Datenschutzbeauftragter
Name Straße Postleitzahl Ort Telefon E-Mail	Name Straße Postleitzahl Ort Telefon E-Mail

Nr.	Verantwortlicher	Betroffene	Zweck der Speicherung	Datenkategorien	Empfänger	Übermittlung an Drittstaaten	Frist zur Löschung	TOMs
1								
2								
3								
4								
5								

Sind Ihnen sämtliche Angaben, die im Verzeichnis aufzuführen sind, bekannt (ja/nein)?

V. Benötigt Ihr Unternehmen einen Datenschutzbeauftragten?

Sind mindestens zehn Personen in Ihrem Unternehmen mit der Datenverarbeitung beschäftigt (nach Köpfen), muss nach Artikel 37 Abs. 2 DS-GVO ein Datenschutzbeauftragter bestellt werden. Es kann ein interner Datenschutzbeauftragter oder ein externer Datenschutzbeauftragter bestellt werden.

Daneben ist ein Datenschutzbeauftragter immer dann vorgeschrieben, wenn besonders sensible Daten, zum Beispiel Gesundheitsdaten, verarbeitet werden und die Verarbeitung dieser sensiblen Daten zur Kerntätigkeit des Unternehmens gehört.

Der Datenschutzbeauftragte überwacht die Datenverarbeitungsprozesse im Unternehmen, unterrichtet und berät die Geschäftsführung. Er hat zudem auf die

Einhaltung des Datenschutzes hinzuwirken. Hierfür muss der Datenschutzbeauftragte die notwendigen Kenntnisse vorweisen können. Die Kontaktdaten des Datenschutzbeauftragten sind der Datenschutzaufsichtsbehörde mitzuteilen.

Müssen Sie aufgrund der vorstehenden Ausführungen einen Datenschutzbeauftragten bestellen (ja/nein)?

VI. Wissen Sie, ob die Rechtmäßigkeit der Datenerhebung gegeben ist?

Ist die Datenverarbeitung in den jeweiligen Verarbeitungsprozessen rechtlich zulässig? Zulässig ist die Datenverarbeitung, wenn entweder eine Einwilligung des Betroffenen vorliegt (siehe Muster in der Anlage), die Datenverarbeitung der Erfüllung eines Vertrages dient oder durch „berechtigte Interessen" des Verantwortlichen legitimiert ist.

So bedarf zum Beispiel die Newsletter-Anmeldung zu Werbezwecken auf einer Webseite der Einwilligung durch den Betroffenen. Bei der Datenverarbeitung im Zusammenhang mit einer Bewerbung bedarf es der Einwilligung nicht, da sie zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Ebenfalls bedarf es keiner Einwilligung im Zusammenhang mit der Vermittlung und Abwicklung von Verträgen.

Wissen Sie, wann eine Einwilligung erforderlich ist und welche berechtigten Interessen für eine rechtmäßige Datenverarbeitung sprechen (ja/nein)?

VII. Ist die Datensicherheit in Ihrem Unternehmen gewährleistet?

Gemäß Artikel 32 GS-GVO sind Maßnahmen zur Datensicherheit zu ergreifen. Hierzu sollte hinsichtlich der jeweiligen Verarbeitungsvorgänge (siehe oben) folgendes geprüft werden:

- Datensparsamkeit: Ist die Speicherung von Daten und deren Verarbeitung tatsächlich notwendig?

- Sind die personbezogenen Daten auf dem neusten Stand? Gibt es Routinen, um die Daten auf den neusten Stand zu bringen?

- Löschfristen: Wie lange werden die Daten benötigt? Wie und wann werden die Daten gelöscht?

- Zugriffsrechte: Wer hat Zugriff auf die Daten? Wer muss notwendigerweise auf die Daten Zugriff nehmen können? Hinweis: Zugriffsberechtigt sind nur die Personen, die für die Verarbeitung und Erfüllung des Zwecks notwendig sind.

- Zugangskontrolle: Wer hat Zugang zu Aktenschränken und Rechnern? Ist der Zugang zu den Bereichen, in denen personbezogene Daten aufbewahrt werden, gewährleistet?

Walderseestr. 14 A
30177 Hannover
http://www.vertriebundrecht.de
Tel.: 0511 66 10 23
Fax.: 0511 66 10 32
eMail: bode@vertriebundrecht.de

- Virensoftware: Ist eine Firewall und ist ein Virenscanner installiert?

Werden die vorgenannten Anforderungen an die Datensicherheit eingehalten (ja/nein)?

VIII. Werden die notwendigen technischen und organisatorischen Maßnahmen (TOMs) ergriffen, um die Integrität, Vertraulichkeit und Verfügbarkeit der Daten zu gewährleisten?

Die Integrität, Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personbezogenen Daten ist zu gewährleisten. Soweit möglich, sollten hierzu personbezogene Daten verschlüsselt werden. Es empfiehlt sich auch die Verschlüsselung von E-Mails. Die EDV Systeme sollten belastbar sein, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sicherstellen zu können. Im Übrigen müssen Verarbeitungsprozesse vor Datenverlusten geschützt werden. Zudem ist eine regelmäßige Überprüfung der Datensicherheit ebenfalls vorgeschrieben. Die technischen und organisatorischen Maßnahmen sollten dokumentiert werden. Hierauf kann dann im Verarbeitungsverzeichnis (siehe oben) verwiesen werden.

Werden die notwenigen TOMs in Ihrem Unternehmen umgesetzt (ja/nein)?

IV. Wissen Sie, ob Sie Auftragsverarbeiter zur Datenverarbeitung einsetzen?

Sie müssen prüfen, ob Dienstleister für Sie personbezogene Daten weisungsgebunden verarbeiten oder ggf. Sie selbst im Auftrag Daten weisungsgebunden verarbeiten (zum Beispiel Webhoster, Lettershop, externe Lohnbuchhaltung). Handelsvertreter sind in der Regel keine Auftragsverarbeiter, da sie nicht weisungsgebunden arbeiten.

Der Auftragsverarbeiter ist die verlängerte Werkbank des Verantwortlichen. Der Verantwortliche bleibt datenschutzrechtlich in der Haftung. Der Auftragsverarbeiter hat ein spezielles Verarbeitungsverzeichnis als Auftragsverarbeiter zu führen.

Mit den Auftragsverarbeitern sind Verträge zu schließen, um sicherzustellen, dass die datenschutzrechtlichen Anforderungen auch vom Auftragsverarbeiter eingehalten werden.

Beauftragen Sie Auftragsverarbeiter und haben Sie schriftliche Verträge mit dem Auftragsverarbeiter abgeschlossen (ja/nein)?

Walderseestr. 14 A
30177 Hannover
http://www.vertriebundrecht.de

Tel.: 0511 66 10 23
Fax.: 0511 66 10 32
eMail: bode@vertriebundrecht.de

V. Kennen Sie Ihre Informationspflichten bei Erhebung der Daten?

Bei der Erhebung von personbezogenen Daten (auf der Website, im Rahmen des Bewerbungsverfahrens, bei der Einstellung von Mitarbeitern, Aufnahme von Kundendaten, Lieferantendaten, Videoüberwachung etc.) hat der Verantwortliche Informationspflichten einzuhalten und eine Datenschutzerklärung dem Betroffenen zur Verfügung zu stellen (siehe Muster in der Anlage).

Dort ist unter anderem aufzuführen, wer der Verantwortliche ist, zu welchem Zweck die Daten erhoben werden, wann sie gelöscht werden und welche Rechte der Betroffene hat.

Verfügen Sie über die notwendigen Datenschutzerklärungen (ja/nein)?

RA Andreas Bode©

Walderseestr. 14 A
30177 Hannover
http://www.vertriebundrecht.de

Tel.: 0511 66 10 23
Fax.: 0511 66 10 32
eMail: bode@vertriebundrecht.de

Einwilligung zu Foto- und Videoaufnahmen

Muster GmbH
Musterstraße 1
1000 Musterstadt

Betreff: Foto- und Videoaufnahmen

Sehr geehrte Damen, sehr geehrte Herren,

wir sind zurzeit damit beschäftigt, die Außendarstellung unseres Unternehmens zu verbessern. In diesem Zusammenhang planen wir, den Internetauftritt zu überarbeiten. Um die Kundenfreundlichkeit zu erhöhen, sollen sämtliche Vertriebsmitarbeiter namentlich und mit einem Lichtbild auf unserer Internetseite aufgeführt werden. Geplant ist auch die Anfertigung eines kleinen Firmenvideos.

Wir bitten Sie, uns bei diesem Vorhaben zu unterstützten. Hierzu benötigen wir Ihre Mithilfe. Wir bitten Sie deshalb um Ihre Einwilligung, Foto- und Videoaufnahmen von Ihnen für unseren Internetauftritt www.mustergmbh.de verwenden zu dürfen.

Die Einwilligung bezieht sich ausschließlich auf die vorgenannte Internetseite. Bitte bedenken Sie, dass Ihr Name und Ihr Foto über Suchmaschinen im Internet recherchiert werden kann.

Die Veröffentlichung soll auf unbestimmte Zeit erfolgen. Die Einwilligungserklärung gilt ab dem Datum der Unterschrift und gilt bis zu dem Zeitpunkt, zudem das Arbeitsverhältnis endet. Anschließend werden die Lichtbilder und Videoaufnahmen, auf denen Sie zu erkennen sind, gelöscht.

Einwilligungserklärung

Name, Adresse

Ich bin damit einverstanden, dass ein Bild von mir im Rahmen von Foto- und Videoaufnahmen sowie mein Name auf der Interseite www.mustergmbH.de veröffentlicht wird.

Ort, Datum
Unterschrift

Verarbeitungsverzeichnis des Verantwortlichen (HV)

Name des Handelsvertreters Straße Postleitzahl Ort Telefon E-Mail	Datenschutzbeauftragter, falls vorgeschrieben

Nr.	Verantwortlicher	Zweck der Speicherung	Betroffene	Datenkategorien	Empfänger	Übermittlung an Drittstaaten	Frist zur Löschung	TOMs
1	s.o.	Anbahnung eines Beschäftigungs-verhältnisses, Bewerbermanagement	Bewerber	Name, Adresse, Zeugnisse, Lebensläufe, Beurteilungen	Geschäftleitung	nein	3 Monate nach Abschluss des Bewerbungsverfahren, mit Einwilligung des Betroffenen 2 Jahre	siehe Sicherheits-konzept
2	s.o	Durchführung von Beschäftigungsverhältnissen	Mitarbeiter	Name, Adresse, Zeugnisse, Lebensläufe, Beurteilungen, Krankentage	intern: Buchhaltung und Geschäftsleitung extern: Sozialversicherungsträger, Krankenkassen, Finanzamt, Steuerberater	nein	nach Ablauf der handels- und steuerrechtlichen Aufbewahrungspflichten, 10 Jahre	siehe Sicherheits-konzept
3	s.o	Vermittlung und Abwicklung von Geschäften	Kunden, ehemalige Kunden, Mitarbeiter der Kunden	Stammdaten, Name, Kontaktdaten, Abrechnungsdaten, Auftragsdaten	vertretene Unternehmen, Lieferanten	nein	nach Ablauf der handels- und steuerrechtlichen Aufbewahrungspflichten, 10 Jahre	siehe Sicherheits-konzept
4	s.o.	Leistungserbringung aus HV-Verträgen	Mitarbeiter vertretener Unternehmen	Stammdaten, Name, Kontaktdaten, Abrechnungsdaten	Buchhaltung, Vertrieb, Geschäftsleitung	nein	nach Ablauf der handels- und steuerrechtlichen Aufbewahrungspflichten, 10 Jahre	siehe Sicherheits-konzept
5.	s.o.	Einkauf, Beschaffung, Abwicklung von Geschäften	Lieferanten, ehemalige Lieferanten, Mitarbeiter der Lieferanten	Stammdaten, Name, Kontaktdaten, Abrechnungsdaten	Buchhaltung, Einkauf, Geschäftsleitung	nein	nach Ablauf der handels- und steuerrechtlichen Aufbewahrungspflichten, 10 Jahre	siehe Sicherheits-konzept
6.	s.o.	Marketing, Marktforschung, Verbesserung der Webseite	Webseiten-besucher	Pseudonymisierte Profile	Vertrieb, Marketingabteilung, Geschäftsleitung	nein	6 Monate	siehe Sicherheits-konzept
7.	s.o	Marketing, Werbung	Interessenten, ehemalige Kunden, potentielle Kunden	Stammdaten, Name, Kontaktdaten, Abrechnungsdaten	Vertrieb, Marketingabteilung, Geschäftleitung	nein	2 Jahre nach Ende der Kundenbeziehung	siehe Sicherheits-konzept

Verpflichtungserklärung zur Wahrung der Vertraulichkeit

Verantwortlicher: Name, Kontaktdaten

Sehr geehrte(r) Frau/Herr.....

aufgrund Ihrer Aufgabenstellung haben Sie im Rahmen Ihrer Tätigkeit Zugang zu personenbezogenen Daten.

Deshalb verpflichte ich Sie auf die Wahrung der Vertraulichkeit personenbezogener Daten nach Art. 5 Abs. 1 f, Art. 32 Abs. 4 Datenschutz-Grundverordnung (DSGVO), zu denen Sie im Rahmen Ihrer Tätigkeit Zugang erhalten oder Kenntnis erlangen.

Es ist Ihnen untersagt, unbefugt personenbezogene Daten zu verarbeiten. Sie dürfen personenbezogene Daten selbst nicht ohne Befugnis verarbeiten. Ferner dürfen Sie anderen Personen diese Daten nicht unbefugt mitteilen oder zugänglich machen.

Diese Verpflichtung besteht auch nach Beendigung Ihrer Tätigkeit fort.

Verstöße gegen die Vertraulichkeit können nach Art. 83 Abs. 4 DSGVO, §§ 42, 43 BDSG sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden.

Was unter der Verarbeitung personenbezogener Daten gemäß DSGVO zu verstehen ist sowie die Strafvorschriften des § 42 BDSG (neu) finden Sie im Merkblatt in der Anlage.

In der Verletzung der Vertraulichkeit kann zugleich eine Verletzung arbeits- oder dienstrechtlicher Schweigepflichten liegen.

Über die Verpflichtung zur Vertraulichkeit und die sich daraus ergebenden Verhaltensweisen wurde ich unterrichtet. Das Merkblatt zur Verpflichtungserklärung habe ich erhalten.

Ort, Datum Unterschrift des Verpflichteten

Merkblatt rechtliche Grundlagen

Art. 4 DSGVO Begriffsbestimmungen

Im Sinne dieser Verordnung sind

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“ = jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.

Strafvorschriften des § 42 DSAnpUG-EU (BDSG-neu)

(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,

   3. ohne hierzu berechtigt zu sein, verarbeitet oder

   4. durch unrichtige Angaben erschleicht

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

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

Technische und organisatorische Maßnahmen der Datensicherheit

Checkliste

Art. 32 DSGVO verpflichtet den Verantwortlichen dazu, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der personenbezogenen Daten zu gewährleisten.

Die nachfolgende Checkliste dient dazu festzustellen, welche Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der personenbezogenen Daten ergriffen werden können. Weitere Maßnahmen, die die Sicherheit erhöhen, können und sollten selbstverständlich zusätzlich ergriffen werden.

1. Zutrittskontrolle

Die Zutrittskontrolle dient dazu, Unbefugte von der Datenverarbeitung und den personenbezogenen Daten fernzuhalten.

Dieses Ziel kann zum Beispiel durch folgende Maßnahmen erreicht werden:

- Alarmanlage
- Videoüberwachung am Eingang
- Empfang und Registrierung der Besucher
- Chipkarten-/Transponder-Schließsystem
- Abschließbare Serverräume
- Auswahl Reinigungspersonal
- Sicherheitsschlösser

2. Zugangskontrolle

Die Zugangskontrolle dient dazu, dass Unbefugte Zugang zu den Datenverarbeitungsanlagen erhalten und Daten lesen, kopieren, verändern oder löschen können.

Zum Beispiel:

- Passwörter
- VPN-Tunnel
- Verschlüsselung
- Anti-Viren-Software
- Firewall
- Benutzerberechtigungen

3. Zugriffskontrolle

Nur Berechtigte sollen Zugriff haben auf die personenbezogenen Daten.

Zum Beispiel:

- Festlegung von Berechtigungen
- Schreddern der Akten
- Festlegung der Administratoren
- Protokollierung von Zugriffen

4. Trennungskontrolle

Trennung von Daten für unterschiedliche Zwecke.

Zum Beispiel:

- physikalische Trennung der Datenbanken

5. Pseudonymisierung

Keine Zuordnung zu einer Person mehr ohne zusätzliche Informationen mehr möglich.

Zum Beispiel:

- physikalische Trennung der Datenbanken
- Trennung der Zuordnungsdaten

6. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Zum Beispiel:

- Verschlüsselung
- VPN
- Übergabeprotokoll

7. Eingabekontrolle

Gewährleistung, dass nachträglich geprüft und festgestellt werden kann, wer die Daten bearbeitet hat.

Zum Beispiel:

- Eingabeprotokolle

8. Verfügbarkeitskontrolle

Maßnahmen zur Verhinderung, dass personenbezogene Daten verloren gehen oder zerstört werden.

Zum Beispiel: :

- Serverräume klimatisiert
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte
- Rauchmelder

9. Wiederherstellbarkeit

Im Störungsfall müssen die Daten wiederhergestellt werden können.

Zum Beispiel:

- Backups

10. Zuverlässigkeit

Gewährleistung der Zuverlässigkeit aller Funktionen des Systems.

Zum Beispiel:

- Unabhängigkeit der Systeme von einander funktionierende Systeme
- Meldung von Fehlfunktionen
- Firewall
- Anti-Viren-Software

Dokumentation
Technische und organisatorische Maßnahmen des Verantwortlichen

Der Verantwortliche bestätigt, dass er folgende technische und organisatorische Maßnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung ergriffen hat:

1. **Zutrittskontrolle**

2. Zugangskontrolle

3. Zugriffskontrolle

4. Trennungskontrolle

5. Pseudonymisierung

6. Transportkontrolle

7. Eingabekontrolle

8. Verfügbarkeitskontrolle

9. Wiederherstellbarkeit

10. Zuverlässigkeit

11. sonstige Maßnahmen

Datum/Unterschrift