


**Datenschutz**

Gefahr/ Risiko	Ist-Zustand	Maßnahme
Unberech- tigte Erhebung von personen- bezogenen Kunden- oder Mitarbeiter- daten	Können die Daten einer konkreten Person zugeordnet werden? <b>Nein</b>	Umgesetzt? <input type="checkbox"/> Die Daten fallen nicht unter BDSG und LDSG.
	Gibt es eine gesetzliche Grundlage oder hat die Person der Erhebung schriftlich zugestimmt? <b>Nein</b>	Umgesetzt? <input type="checkbox"/> Die Daten sind unverzüglich zu löschen, da deren Erhebung unzulässig war.
	Sind die Daten überprüfbar und stammen sie aus einer vertrauenswürdigen Quelle? <b>Nein</b>	Umgesetzt? <input type="checkbox"/> Speichern Sie nur Daten, die nachweisbar korrekt sind.
	Sind die erhobenen personenbezogenen Daten falsch? <b>Ja</b>	Umgesetzt? <input type="checkbox"/> Berichtigen Sie die Daten.
Unberechtigte Speicherung von Personen- bezogenen Daten	Bestreitet die Person die Richtigkeit und lässt sich weder die Korrektheit noch die Fehlerhaftigkeit der Daten feststellen? <b>Ja</b>	Umgesetzt? <input type="checkbox"/> Sperren Sie die Daten und versehen Sie die Sicherungsbänder mit einem Hinweis auf die Sperre.
	Ist die Zweckbindung weggefallen? <b>Ja</b>	Umgesetzt? <input type="checkbox"/> Löschen Sie die Daten.
Unberech- tigter Zugriff auf personen- bezogene Daten	Dürfen nur berechtigte Benutzer auf die Daten zugreifen und diese modifizieren? <b>Nein</b>	Umgesetzt? <input type="checkbox"/> Richten Sie Zugriffsberechtigungen ein, die Sie überprüfen und dokumentieren.
	Können die Daten unbefugt gelesen, kopiert, verändert oder entfernt werden? (Zugriffskontrolle) <b>Ja</b>	Umgesetzt? <input type="checkbox"/> Ermöglichen Sie einen Zugriff nur mit Benutzername und Passwort und verschlüsseln Sie die Daten.

Unkontrollierter Datenabfluss


Sind die Benutzer auf das BDSG/LDSG verpflichtet und auf die Folgen einer Pflichtverletzung hingewiesen worden?

Nein

Umgesetzt?    
Verpflichten Sie die Benutzer *schriftlich* auf den Datenschutz.


Wird Unbefugten der Zutritt zu EDV-Anlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt und werden EDV-Systeme nicht von Unbefugten genutzt? (Zutrittskontrolle)

Nein

Umgesetzt?    
Sichern Sie den Zugang zu EDV Räumen und gewähren Sie den Zugang nur berechtigten Personen.


Gibt es ein Verfahrnsverzeichnis?

Nein

Umgesetzt?    
Erstellen Sie umgehend ein Verfahrnsverzeichnis mit den laut § 4e Satz 1 BDSG geforderten Inhalten. Wichtige Informationen zur Erstellung des Verfahrnsverzeichnis finden Sie im BITKOM-Leiftaden : [http://www.bitkom.org/files/documents/BITKOM\\_Verfahrnsverzeichnis\\_V\\_2.0.pdf](http://www.bitkom.org/files/documents/BITKOM_Verfahrnsverzeichnis_V_2.0.pdf)


Hat der Betrieb mehr als 9 Mitarbeiter, die personenbezogene Daten verarbeiten und ist kein Datenschutzbeauftragter bestellt?

Nein

Umgesetzt?    
Verfahrnsverzeichnis dem Landesdatenschutzbeauftragten senden.


Hat der Betrieb einen betrieblichen Datenschutzbeauftragten bestellt?(Bei mehr als 9 Mitarbeitern, die personenbezogene Daten verarbeiten)

Nein

Umgesetzt?    
Ernennen Sie einen Datenschutzbeauftragten.

Kann nachvollzogen werden, ob und von wem personenbezogene Daten in EDV-Systeme eingegeben, verändert oder entfernt worden sind? (Eingabekontrolle)


Nein

Umgesetzt?    
Führen Sie ein Trackingsystem ein.

Fehlender Manipulationsschutz datenschutzrelevanter Informationen


Sind die Daten wieder auffindbar, nachvollziehbar, unveränderbar und fälschungssicher gespeichert?

Nein

Umgesetzt?    
Sorgen Sie dafür, dass Daten qualifiziert digital signiert werden. (Weitere Infos unter:[http://netzwerk.bistech.de/datadir/server-1/materials/material\\_180/dig\\_signatur\\_dina3.pdf](http://netzwerk.bistech.de/datadir/server-1/materials/material_180/dig_signatur_dina3.pdf))

Sind die Daten gegen zufällige Zerstörung oder Verlust geschützt? (Verfügbarkeitskontrolle)


Nein

Umgesetzt?    
Richten Sie regelmäßige Backups ein und treffen Sie Vorkehrungen gem. Anlage zu §9 BDSG.

Personenbezogene Daten können von Unberechtigten gelesen bzw. bearbeitet werden

Werden zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet?

Nein


Umgesetzt?    
Verarbeiten Sie Daten mit unterschiedlichem Verwendungszweck organisatorisch und technisch getrennt.

Personen-  
bezogene  
Daten können  
unberechtigt  
erfasst  
und zur  
Mitarbeiter-  
überwachung  
verwendet  
werden

Daten können  
leicht  
abgehört  
werden

Werden personenbezogene Daten kopiert (vervielfältigt)?

Ja

Umgesetzt?   
Verschlüsseln Sie die kopierten Daten auf der Festplatte des Kopierers. Die Platte ist vor dem Ausbau zu löschen. Überzählige Papierkopien oder Fehlkopien sollten Sie schreddern.


Werden Unterlagen bei Ihnen digital (z.B. in einem Dokumentenmanagement system- DMS-) gespeichert?

Ja

Umgesetzt?   
Richten Sie Zugriffsrechte gemäß Anlage zu §9 BDSG ein.


Arbeiten Mitarbeiter von zu Hause aus?

Ja

Umgesetzt?   
Schließen Sie eine Vereinbarung zur Nutzung eines Telearbeitsplatzes und stellen Sie die Einhaltung der Vereinbarung sowie die Datensicherheit der Verbindung sicher.


Erfassen Sie Smartphone-Daten?

Ja

Umgesetzt?   
Schließen Sie eine Vereinbarung, welche Sicherheitsmaßnahmen, Datenübertragung, -trennung, -sicherung und -löschung, Wartung, Reparatur, Nutzung durch andere Personen etc. regelt.


Erfassen Sie Geo-Daten Ihrer Mitarbeiter (Ortung)?

Ja

Umgesetzt?   
Schließen Sie eine Vereinbarung, welche die Erfassung von Geodaten regelt, da die Datenverarbeitung ohne Vereinbarung unzulässig ist.


Verwenden Sie RFID-Chips?

Ja

Umgesetzt?   
Machen Sie die Nutzung kenntlich und stellen Sie ein Auslesegerät zur Verfügung.


Setzen Sie Videokameras oder WebCams ein?

Ja

Umgesetzt?   
Sie benötigen eine Vereinbarung und müssen die Nutzung kenntlich machen.


Benutzen Sie ein schnurloses (DECT-) Telefon?

Ja

Umgesetzt?   
Sie dürfen keine personenbezogenen Daten über das Telefon übermitteln.

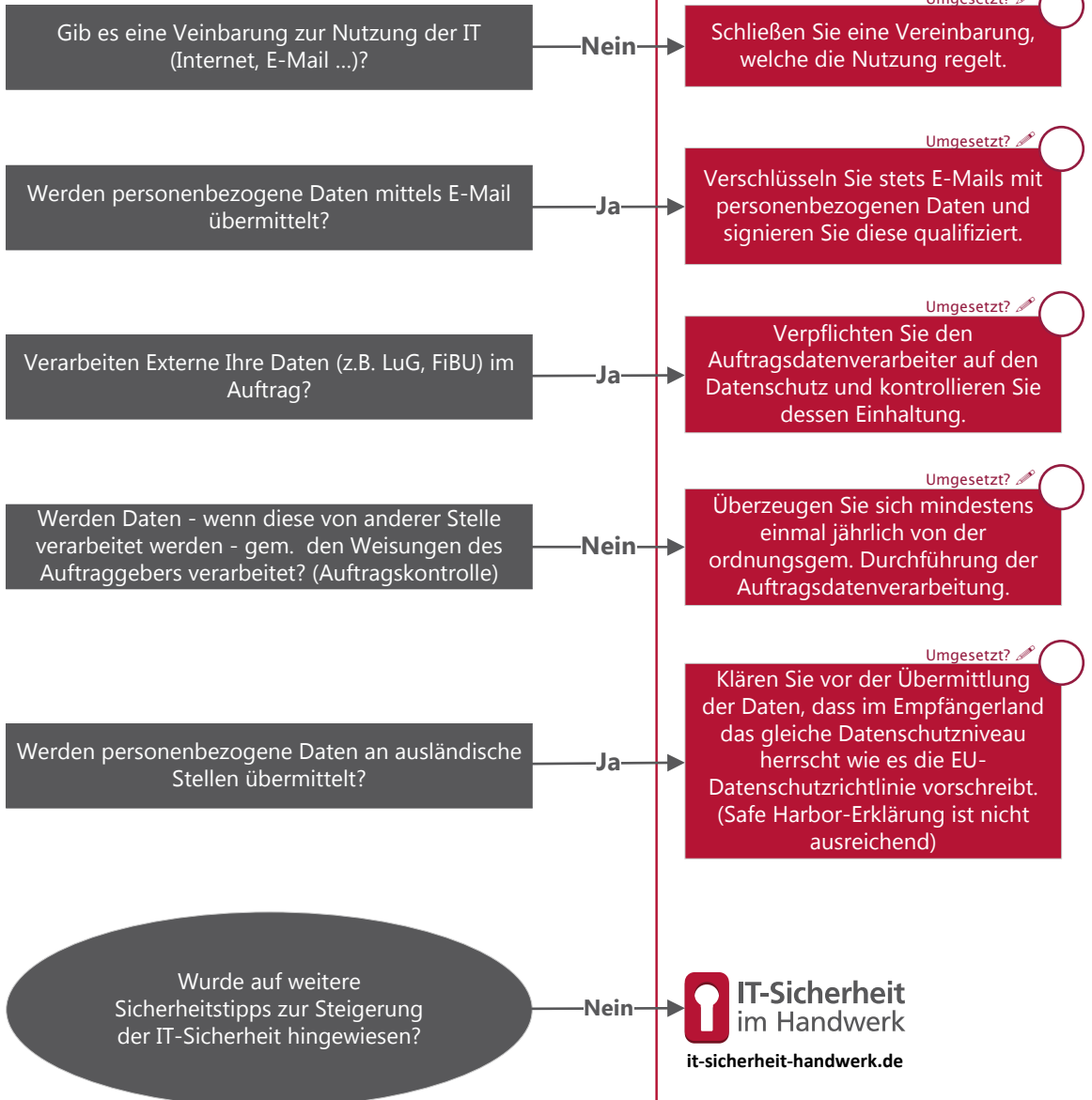
Benutzen Sie ein VoIP-Telefon?

Ja

Umgesetzt?   
Die Kommunikation sollte nur verschlüsselt erfolgen. Sie dürfen personenbezogenen Daten über das Telefon nur verschlüsselt übermitteln.

Daten können unberechtigt gelesen und erfasst werden

Daten können unberechtigt gelesen und verwendet werden



**TASK FORCE**  
**IT-SICHERHEIT IN DER WIRTSCHAFT**  
Mehrwert und Schutz für Rechner.

**Task Force „IT-Sicherheit in der Wirtschaft“**  
Die Task-Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task-Force und ihren Angeboten sind unter:

[www.it-sicherheit-in-der-wirtschaft.de](http://www.it-sicherheit-in-der-wirtschaft.de) abrufbar

[www.it-sicherheit-handwerk.de](http://www.it-sicherheit-handwerk.de)



itb - Institut für Technik der Betriebsführung im Deutschen Handwerksinstitut e.V.



Heinz-Piest-Institut für Handwerkstechnik an der Leibniz Universität Hannover



Handwerkskammer Rheinessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur



if(is) - Institut für Internet-Sicherheit der Westfälischen Hochschule