IT-Sicherheit im Handwerk

Checkliste IT-Sicherheit

Gefördert durch:

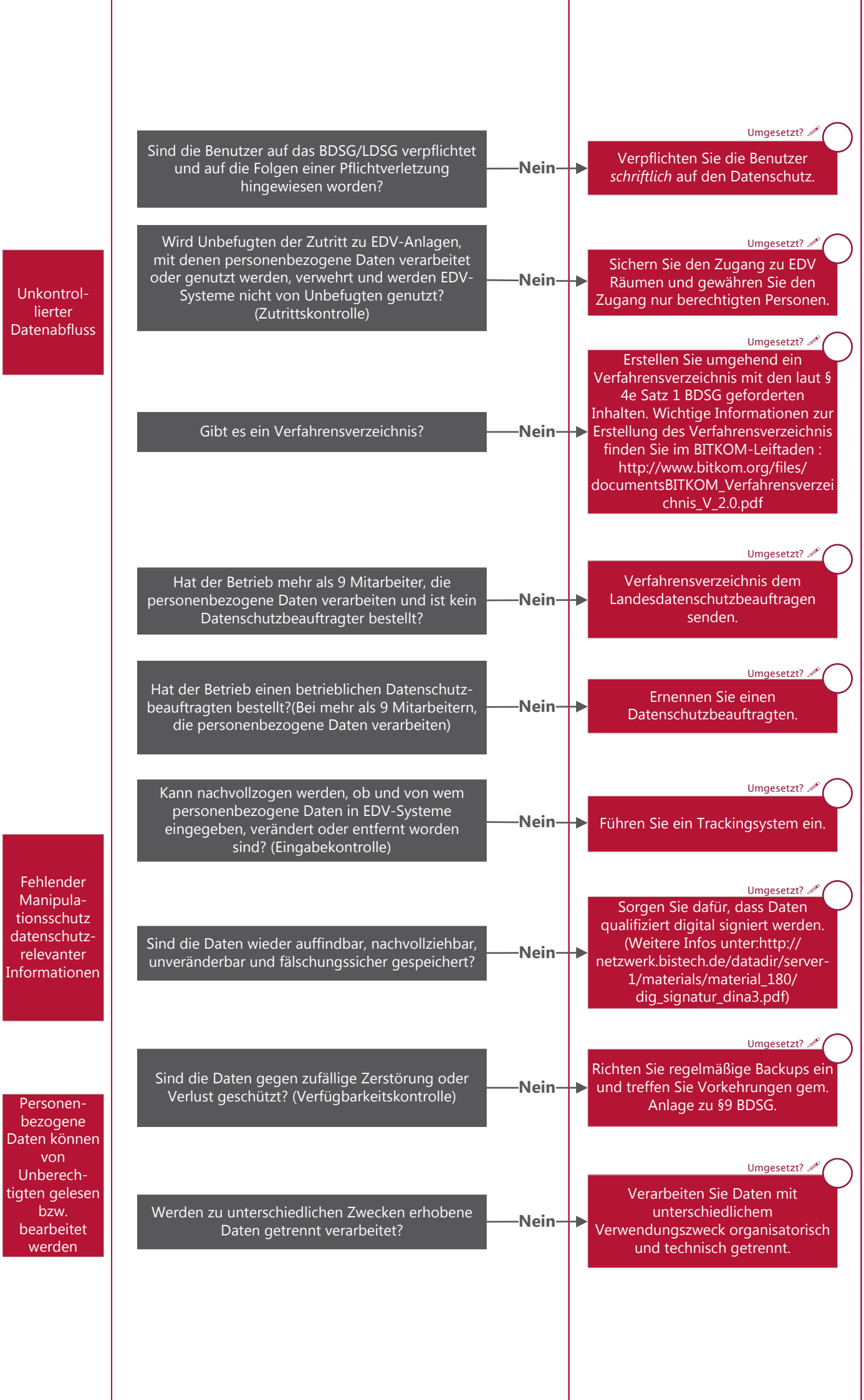
Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

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

Datenschutz

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


Unkontrol-
lierter
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 Verfahrensverzeichnis?
Nein
Umgesetzt?
Erstellen Sie umgehend ein Verfahrensverzeichnis mit den laut § 4e Satz 1 BDSG geforderten Inhalten. Wichtige Informationen zur Erstellung des Verfahrensverzeichnis finden Sie im BITKOM-Leiftaden : http://www.bitkom.org/files/documentsBITKOM_Verfahrensverzeichnis_V_2.0.pdf
Hat der Betrieb mehr als 9 Mitarbeiter, die personenbezogene Daten verarbeiten und ist kein Datenschutzbeauftragter bestellt?
Nein
Umgesetzt?
Verfahrensverzeichnis dem Landesdatenschutzbeauftragen senden.
Hat der Betrieb einen betrieblichen Datenschutz-beauftragten bestellt?(Bei mehr als 9 Mitarbeitern, die personenbezogene Daten verarbeiten)
Nein
Umgesetzt?
Ernennen Sie einen Datenschutzbeauftragten.
Fehlender
Manipula-
tionsschutz
datenschutz-
relevanter
Informationen
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.
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)
Personen-
bezogene
Daten können
von
Unberech-
tigten gelesen
bzw.
bearbeitet
werden
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.
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

Werden personenbezogene Daten kopiert (vervielfältigt)? — Ja → 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. Umgesetzt?

Werden Unterlagen bei Ihnen digital (z.B. in einem Dokumentenmanagement system- DMS-) gespeichert? — Ja → Richten Sie Zugriffsrechte gemäß Anlage zu §9 BDSG ein. Umgesetzt?

Arbeiten Mitarbeiter von zu Hause aus? — Ja → Schließen Sie eine Vereinbarung zur Nutzung eines Telearbeitsplatzes und stellen Sie die Einhaltung der Vereinbarung sowie die Datensicherheit der Verbindung sicher. Umgesetzt?

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

Erfassen Sie Geo-Daten Ihrer Mitarbeiter (Ortung)? — Ja → Schließen Sie eine Vereinbarung, welche die Erfassung von Geodaten regelt, da die Datenverarbeitung ohne Vereinbarung unzulässig ist. Umgesetzt?

Verwenden Sie RFID-Chips? — Ja → Machen Sie die Nutzung kenntlich und stellen Sie ein Auslesegerät zur Verfügung. Umgesetzt?

Setzen Sie Videokameras oder WebCams ein? — Ja → Sie benötigen eine Vereinbarung und müssen die Nutzung kenntlich machen. Umgesetzt?

Daten können leicht abgehört werden

Benutzen Sie ein schnurloses (DECT-) Telefon? — Ja → Sie dürfen keine personenbezogenen Daten über das Telefon übermitteln. Umgesetzt?

Benutzen Sie ein VoIP-Telefon? — Ja → Die Kommunikation sollte nur verschlüsselt erfolgen. Sie dürfen personenbezogenen Daten über das Telefon nur verschlüsselt übermitteln. Umgesetzt?

Daten können unberechtigt gelesen und erfasst werden

Gib es eine Veinbarung zur Nutzung der IT (Internet, E-Mail ...)? — Nein → Schließen Sie eine Vereinbarung, welche die Nutzung regelt. (Umgesetzt?)

Werden personenbezogene Daten mittels E-Mail übermittelt? — Ja → Verschlüsseln Sie stets E-Mails mit personenbezogenen Daten und signieren Sie diese qualifiziert. (Umgesetzt?)

Verarbeiten Externe Ihre Daten (z.B. LuG, FiBU) im Auftrag? — Ja → Verpflichten Sie den Auftragsdatenverarbeiter auf den Datenschutz und kontrollieren Sie dessen Einhaltung. (Umgesetzt?)

Daten können unberechtigt gelesen und verwendet werden

Werden Daten - wenn diese von anderer Stelle verarbeitet werden - gem. den Weisungen des Auftraggebers verarbeitet? (Auftragskontrolle) — Nein → Überzeugen Sie sich mindestens einmal jährlich von der ordnungsgem. Durchführung der Auftragsdatenverarbeitung. (Umgesetzt?)

Werden personenbezogene Daten an ausländische Stellen übermittelt? — Ja → Klären Sie vor der Übermittlung der Daten, dass im Empfängerland das gleiche Datenschutzniveau herrscht wie es die EU-Datenschutzrichtlinie vorschreibt. (Safe Harbor-Erklärung ist nicht ausreichend) (Umgesetzt?)

Wurde auf weitere Sicherheitstipps zur Steigerung der IT-Sicherheit hingewiesen? — Nein → IT-Sicherheit im Handwerk
it-sicherheit-handwerk.de

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 abrufbar

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 Rheinhessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur

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