In 7 Schritten zu EU-DSGVO-Verfahrens-handbuch & Co

Wie verspeist man einen Elefanten?
In kleinen Häppchen!

sphinx
MASTERING THE GAP

In 7 Schritten zu EU-DSGVO-Verfahrenshandbuch & Co

Wie verspeist man einen Elefanten? – In kleinen Häppchen!

Gründe gibt es viele, sich nicht mit langweiliger Dokumentation zu beschäftigen. Doch die DSGVO ist in dem Punkt ganz klar:

Personenbezogene Daten und deren Verarbeitungen müssen dokumentiert werden.

Dieser Leitfaden hilft in 7 Schritten, die DSGVO relevanten Dokumente noch rechtzeitig fertigzustellen. Damit Sie auch nach dem 25.5.2018 ruhig schlafen können!

SCHRITT 1: BETROFFENE DATEN ERHEBEN

Welche Daten werden von Mitarbeitern, Kunden, Lieferanten oder Geschäftspartnern gespeichert? Sind auch „besonders sensible Daten" dabei wie z.B. Gesundheitsdaten oder Religionsbekenntnis?

Wie gehen wir vor?
Das ist nicht ganz einfach und klingt aufwändig, kann aber durch automatisiertes Durchsuchen von Datenbeständen und geführtes Einbeziehen wissender Mitarbeiter gut unterstützt werden. Personenbezogene Daten werden einerseits von Applikationen verwaltet oder sind als identifizierbare Datenbestände (Dateien) auffindbar.

Ergebnis:

Die Liste der Daten, die in Ihrem Unternehmen von der DSGVO betroffen sind.

SCHRITT 2: VERARBEITUNGEN BESCHREIBEN

Welche Verarbeitungen werden mit den in Schritt 1 identifizierten Daten durchgeführt?

- Wer ist für welche Daten verantwortlich
- Für welchen Zweck werden welche Daten gespeichert
- Was genau passiert mit welchen Daten (Art der Verarbeitung)
- Wie lange werden welche Daten gespeichert und warum
- Wer hat Zugriff auf die Daten und an wen werden sie weitergegeben

Wie gehen wir vor?
Jetzt beginnt die Hauptarbeit! Eine gute Vorlage für das Verfahrenshandbuch finden Sie z.B. als Muster bei der WKO. Wir empfehlen jedoch, hier ein paar Euro in eine Software-Lösung zu investieren. Das lohnt sich: Sie werden durch die Fragen gut geführt und mehrere Leute können gleichzeitig daran arbeiten. So können Sie auch einen DSGVO-Kundigen von extern hinzuziehen, der aktiv mitarbeitet oder den Fortschritt verfolgt und Tipps gibt. Auch spätere Anpassungen sind viel leichter und das Verfahrenshandbuch kann immer auf dem letzten Stand gehalten werden.

Ergebnis:

Das Verfahrenshandbuch (Verzeichnis der Verarbeitungstätigkeiten) mit allen vorgeschriebenen Inhalten.

SCHRITT 3: RICHTIGE REAKTION BEI ANFRAGEN VON BETROFFENEN FESTLEGEN

Was muss im Anlassfall konkret geschehen, wenn ein Betroffener eines seiner folgenden Rechte einfordert:

- Informationspflicht
- Auskunftsrecht
- Recht auf Berichtigung
- Recht auf Löschung („Recht auf Vergessenwerden")
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

Wie gehen wir vor?
Für die Erhebung dieser Informationen braucht man mindestens eine Person, die sich mit den Abläufen in der Firma auskennt und eine, die mit den IT-Systemen gut vertraut ist. Moderierte Intensiv-Workshops in Kombination mit „Hausaufgaben" für diese Kollegen bringen aus unserer Erfahrung am raschesten die gewünschten Ergebnisse.

Ergebnis:

- Prozessbeschreibungen für den DSGVO-konformen Ablauf für jede dieser Anfragen
- Arbeitsanweisungen und Schulung für die verantwortlichen Mitarbeiter

SCHRITT 4: IT-ANWENDUNGEN & IT-SYSTEME AUF DSGVO-KONFORMITÄT UNTERSUCHEN

Inwieweit unterstützen die vorhandenen IT-Anwendungen die DSGVO Vorgaben?

- Welche Anwendungen sind im Einsatz
- Wie werden die Betroffenenrechte mit diesen Anwendungen verwirklicht (z.B. wie kann man die Daten sauber löschen)
- Gibt es „Office-Applikationen" (Word, Excel, …), welche personenbezogene Daten verarbeiten, die oft verstreut auf den Filesystemen „herumliegen"

Wie gehen wir vor?
Auflistung der DSGVO relevanten Funktionen in einem Applikationskatalog. Gleichzeitig wird überprüft, in welche Maße die vorhandenen Applikationen die DSGVO-Personenrechte unterstützen.

Ergebnis:

Eine Liste der Applikationen, welche DSGVO-konform sind und welche nicht. Dadurch können die Investitionen für Applikations-Versionen transparent gemacht werden, um sie DSGVO konform zu machen.

SCHRITT 5: RICHTIGE REAKTION BEI MISSBRAUCH DER DATEN FESTLEGEN

Wenn Daten gestohlen werden, ist rasches Handeln angesagt, denn die DSGVO schreibt enge Fristen vor. Was ist zu tun?

- Meldung an die Aufsichtsbehörde (Muster)
- Meldung an die Betroffenen (Muster)

Wie gehen wir vor?
Als Basis dient eine geeignete Vorlage (Anwalt, WKO, …), die an das eigene Unternehmen angepasst wird.
Am Wichtigsten ist die Erstellung einer Checkliste oder Arbeitsanweisung sowie die Schulung der Mitarbeiter, die an der Analyse und Aufarbeitung eines Datendiebstahl involviert sein werden. Sie müssen im Anlassfall unter Stress schnell und richtig reagieren können.

Ergebnis:

- Prozessbeschreibungen für die DSGVO-relevanten Meldungen
- Arbeitsanweisung und Schulung für verantwortliche Mitarbeiter
- Definition von Maßnahmen (technisch, organisatorisch), um das Risiko für solche Vorfälle zu senken

SCHRITT 6: SICHERHEIT DER MOBILEN ENDGERÄTE ÜBERPRÜFEN

Wie sicher sind Laptops, Tablets, Handys & Co und wie kann technisch und organisatorisch sichergestellt werden, unerlaubten Zugriff auf personenbezogene Daten zu verhindern?

Wie gehen wir vor?
Anlegen eines Software- und Datenverzeichnis mit Schwerpunkt auf Sicherheitsfunktionen.

Ergebnis:

- Definition von Maßnahmen (technisch, organisatorisch), um das Risiko für unerlaubte Zugriffe oder unbeabsichtigten Datenverlust zu senken
- Zeitplan für die Umsetzung

SCHRITT 7: SPEZIALFÄLLE PRÜFEN

Welche Spezialfälle treffen auf Ihr Unternehmen zu, wo weitere Dokumente im Sinne der DSGVO vorhanden sein müssen? Dies können z.B. Gesundheitsdaten oder die Art der Verarbeitung (Videoaufzeichnungen, Profiling, ...) sein.

Wie gehen wir vor?
Es werden die in Schritt 1 und 2 erhobenen Informationen so kombiniert, dass dadurch mögliche Spezialfälle sichtbar werden. Beispiele dafür wären die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten, oder ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss.

Ergebnis:

Eines oder mehrere der folgenden Dokumente:

- Dokumentation der Einwilligungserklärungen
- Dokumentation der Sicherheitsmaßnahmen
- Dokumentation der Risikoabschätzung
- Dokumentation von Arbeitsanweisungen
- Mustervertrag für die Auftragsverarbeitung
- Dokumentation der Geheimhaltungspflicht

ZUSAMMENFASSUNG

Das 7-Punkte-Programm von sphinx ist eine pragmatische Vorgehensweise, die einfache Methoden, bewährte Vorlagen, eine schlanke Software-Lösung und Mitarbeiter-Schulung umfasst. Damit sind Sie im Sinne der DSGVO bezüglich aller Dokumentationspflichten „auf der sicheren Seite".

Im Zuge des 7-Punkte-Programmes werden Sie und Ihre Mitarbeiter zusätzliche Erkenntnisse gewinnen, die dem Unternehmen in Form von Verbesserungsvorschlägen und neuen Ideen viel nützen können:

- Verbesserung von Abläufen sorgt für höhere Effizienz und Transparenz
- Mehr Informationen aus vorhandenen Daten zu ziehen hilft bei der laufenden Verbesserung der Dienstleistung oder der Produkte
- „Ausmisten" unnötiger Daten oder Verarbeitungen schafft Luft für Neues und entlastet die Mitarbeiter
- Schaffen der Awareness bei Mitarbeitern ist eine gute Vorbeugemaßnahme gegen Datenverlust durch Angriffe von innen und außen
- Erhöhen der Betriebssicherheit senkt das Risiko von Geschäftsausfällen