Datenschutz @ PHOENIX CONTACT

EU-DSGVO

Die EU-DSGVO
im Industrieunternehmen

Stellenwert, Prioritäten in der Umsetzung, konkrete TODOs

Helmut Karnath, Datenschutzbeauftragter

PHOENIX CONTACT
INSPIRING INNOVATIONS

Datenschutz @ Phoenix Contact

Die Person

Helmut Karnath, Datenschutzbeauftragter

Vorstellung

Helmut Karnath

- Mitarbeiter im Phoenix Contact Headquarter in Blomberg
- Seit 2012 Datenschutzbeauftragter (DSB) für deutsche Gesellschaften der Phoenix Contact Unternehmensgruppe

PHOENIX CONTACT
INSPIRING INNOVATIONS

Datenschutz @ Phoenix Contact

Das Unternehmen

Phoenix Contact

PHOENIX CONTACT
INSPIRING INNOVATIONS

Von der Reihenklemme zum Vollsortiment

Reihenklemmen

Leiterplattenanschluss

Industriestecker

Überspannungsschutz

Signalanpassung

Automatisierung

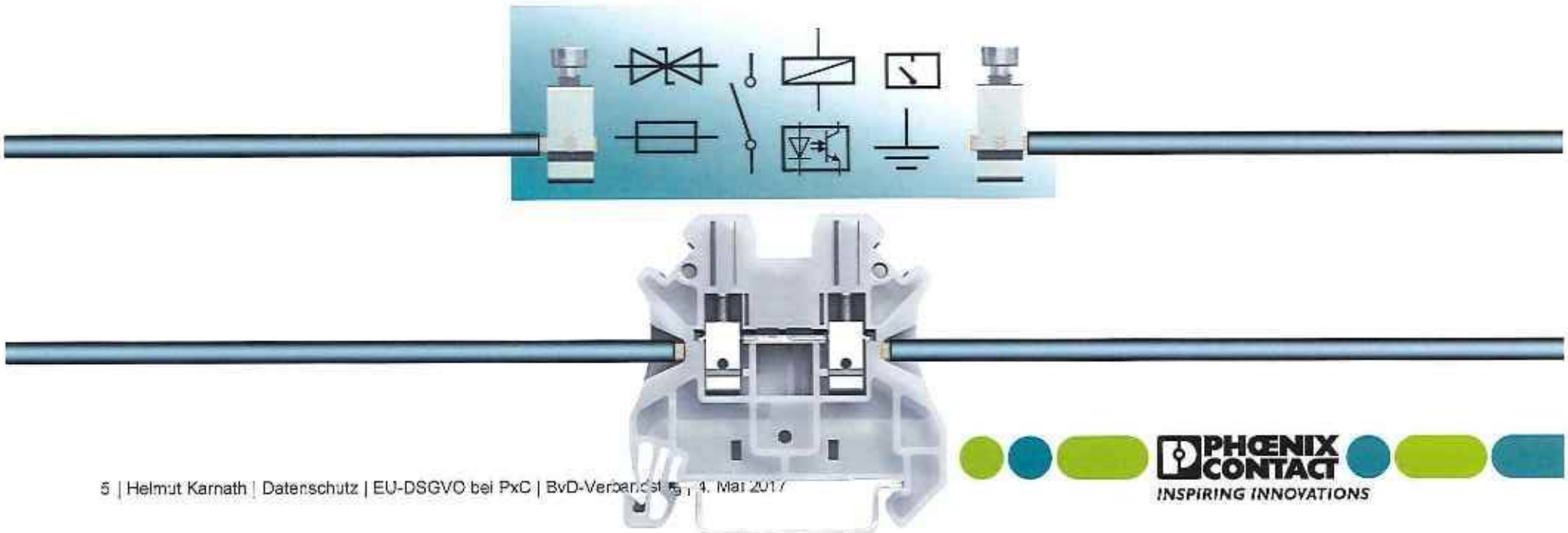
Printanschlüsse

Ü-Schutz

Mehrstockklemmen

Federkrafttechnik

IDC-Technik

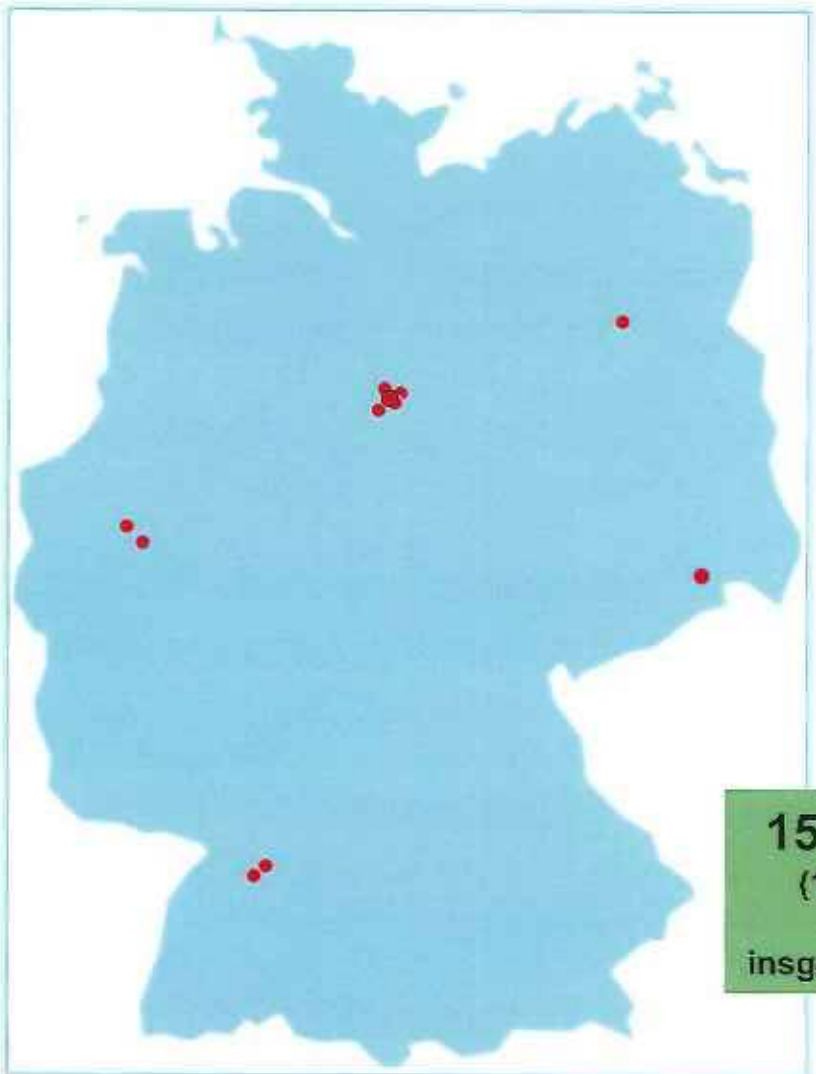


PHOENIX CONTACT
INSPIRING INNOVATIONS

Mitarbeiter/Umsatz

PHOENIX CONTACT
INSPIRING INNOVATIONS

PHOENIX CONTACT Gruppe in Deutschland



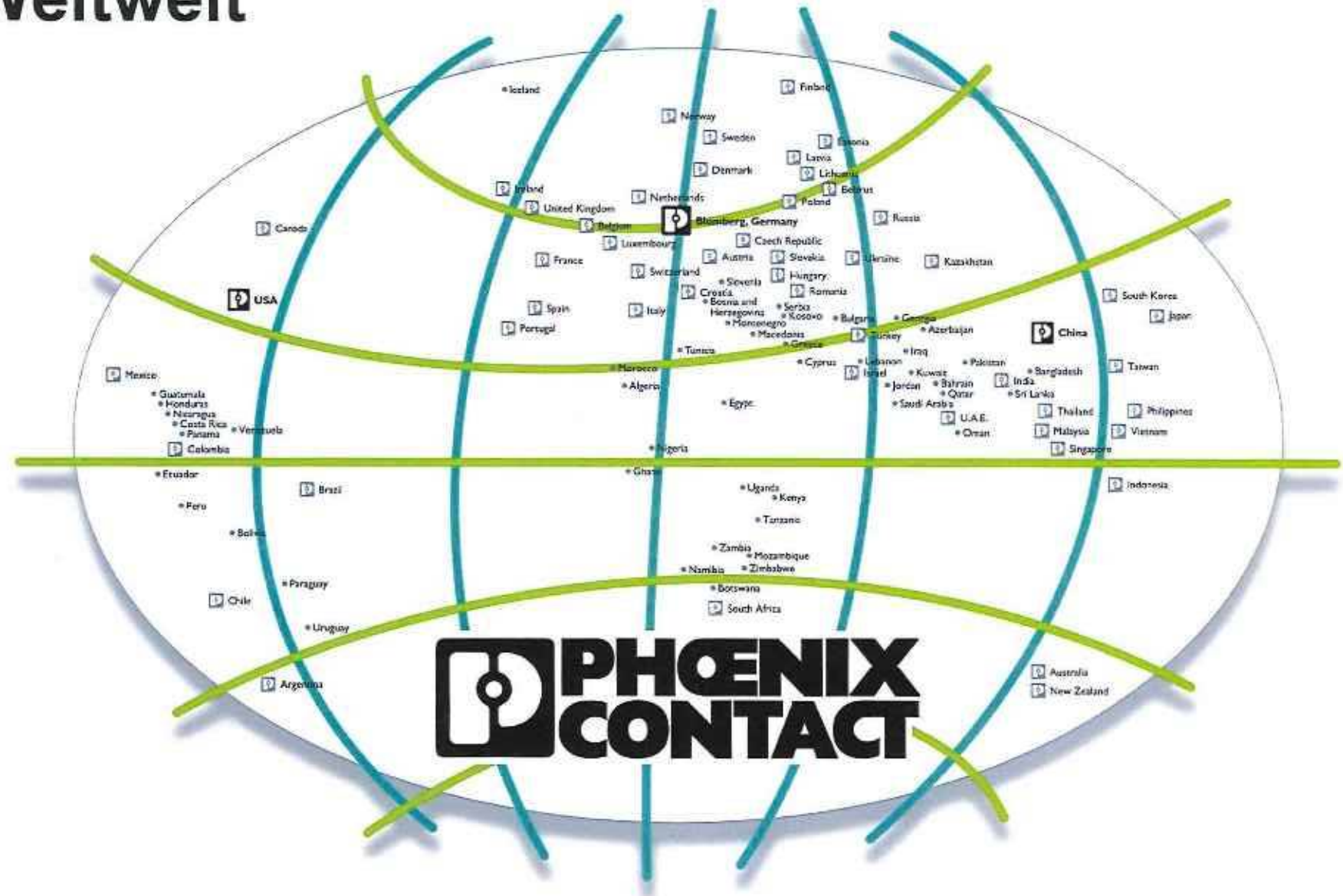
PHOENIX CONTACT GmbH & Co. KG
Headquarter, Blomberg

15 Gesellschaften
(10 – 5.000 Mitarbeiter)

insges. 7.500 Mitarbeiter in D

INSPIRING INNOVATIONS

Weltweit



PHOENIX CONTACT
INSPIRING INNOVATIONS

Datenschutz @ Phoenix Contact

Die EU-DSGVO

Stellenwert, konkrete TODOs, Prioritäten in der Umsetzung

PHOENIX CONTACT
INSPIRING INNOVATIONS

Warum (jetzt) was tun?

PHOENIX CONTACT
INSPIRING INNOVATIONS

Warum (jetzt) was tun?

- **Die mögliche *Bußgeldhöhe* tut nun zu weh, um ignoriert zu werden!**
- **Bußgeldtatbestände sind stark ausgeweitet worden**
- **Analog zum Kartellrecht werden sich die Bußgeldhöhen in den EU-Ländern auf *hohem Niveau* angleichen!**
- **Bußgeldpflicht** „...in jedem Einzelfall wirksam, verhältnismäßig und abschreckend..."
- Das Risiko anlassloser Kontrollen nimmt (vorerst) nicht zu.
  Die Risikowahrscheinlichkeit bei Industrieunternehmen (B2B) „erwischt" zu werden ist aus *diesem* Grund gering, wird aber steigen! Warum?
  - Mitarbeiter, Geschäftspartner und Verbraucher werden immer sensibler
  - Datenschutzverstöße sind nun abmahnfähig
  - Verbandsklagen sind nun zugelassen
  - Von „außen" feststellenbare Datenschutzverstöße werden zunehmend von den Datenschutzbehörden geprüft (Websites, Apps)
  - Der Reiz des hohen Bußgeldes und die Beweislastumkehr wird motivieren! (Abmahnanwälte, Betroffene, Mitbewerber, Datenschutzbehörden, ...)
  - **DS-Behörden müssen sich zukünftig EU-weit abstimmen (Kohärenzpflicht)**
  - **Entwicklung analog Kartellrecht**

Aktiv sein: JA! ... aber womit?

- **Am Ball bleiben!**
  Aktuelle Entwicklung der Rechtsauffassungen
  zur EU-DSGVO und zum BDSGneu permanent verfolgen.

- **Individuelle ToDo-Liste erstellen!!!**
  - WAS: Themen erkennen und benennen (GAP-Analyse)
  - WANN: Themen priorisieren nach Risiko (►Außenwirkung, ►Bußgeld)
    und erforderlicher Vorlaufzeit (zeitlicher ►Dringlichkeit)
  - WER: Themen Personen zuordnen (DSB/DSKs, IT, Fachabteilungen)

- **ToDos aktiv angehen!**

Was sind meine „Basis“-Aktivitäten?

- **Wie informiere ich mich?** u. a., durch
  - diverse Newsletter, Fachzeitschriften, Eigenrecherche im Web
  - Orientierungshilfen der Datenschutzbehörden und Verbände
  - Teilnahme an Infoveranstaltungen, Schulungen und Kongressen
  - Teilnahme an GDD / BvD-Erfakreisen

meine Intention: Gefühl für die Notwendigkeiten bekommen!!!

bei u. a. :

- Rechenschaftspflicht/Accountability
- Datenschutzfolgenabschätzung
- Informationspflichten
- Privacy by design/default
- Datenübertragbarkeit
- ...

Ziel: Pragmatische aber rechtskonforme Lösungen finden!

Linkliste für einen ersten! Überblick

- Bitkom
  Was muss ich wissen zur EU-Datenschutz Grundverordnung
  https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/160909-EU-DS-GVO-FAQ-03.pdf

- AWV – Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.
  EU-Datenschutz-Grundverordnung (DSGVO) – Die neuen europäischen Datenschutzvorschriften – wichtige Änderungen und ihre Auswirkungen auf Wirtschaft und Verwaltung
  http://www.awv-net.de/upload/online-dokumente/04651_Broschre_zur_DSGVO.pdf

- RA Tim Wybitul, Dr. Oliver Draf LL.M.
  Projektplanung und Umsetzung der EU-Datenschutz-Grundverordnung im Unternehmen
  http://hoganlovells-blog.de/wp-content/uploads/2016/09/BB-Beitrag-zur-Projektplanung-zur-Umsetzung-der-DSGVO.pdf

- Forum Privatheit
  White Paper „Datenschutz-Folgenabschätzung"
  https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf

- Datakontext (Gola/Jaspers/Müthlein/Schwartmann)
  Datenschutz-Grundverordnung im Überblick (kostenpflichtig)
  http://www.datakontext.com/shop/Datenschutz/Praxis/EU-Datenschutz-Grundverordnung-im-UEberblick-Softcover.html

- RA Hansen-Oest
  Webinaraufzeichnung: Wie Unternehmen sich jetzt schon auf die DSGVO vorbereiten sollten
  https://www.datenschutz-guru.de/2016/08/webinaraufzeichnung-wie-unternehmen-sich-schon-jetzt-auf-die-dsgvo-vorbereiten-sollten/

Was kommt nach dem WAS?

PHOENIX CONTACT
INSPIRING INNOVATIONS

...vom WAS zum WIE...

WIE...

- ...müssen die Nachweise (Accountability) erbracht werden und in welcher Granularität
- ...muss eine konkrete Checkliste aussehen, um Privacy by design/default zu erfüllen
- ...muss ein neuer ADV-Muster(hybrid)vertrag aussehen
- ...komme ich der Transparenzpflicht gegenüber Mitarbeiter/Kunden/Geschäftspartnern/etc. nach (Form, Kanal)
- ...muss eine Datenschutzfolgenabschätzung konkret gemacht werden (und für welche Verarbeitungen)
- ...könnte eine Rahmenbetriebsvereinbarung zur DSGVO/BDSGneu aussehen
- ... ...

Was kommt auf uns in D zu? (wesentliches Δ)

- ▲ **Rechenschaftspflicht (Accountability)**
- ▲ **Privacy by design/default**
- ▲ **Sperr- / Löschpflicht** pbDaten (+ Right to be forgotten)
- **Informations-/Transparenzpflicht** (ggü. Mitarbeitern, Geschäftspartn./Kunden)
- **Auskunftspflicht** (+ Datenübertragbarkeit)
- **IT-Sicherheit** (auf Basis Risikoanalyse mit Fokus Betroffener)
- **Datenschutz-Folgenabschätzungen** (auf Basis Risikoanalyse)
- **Meldepflicht bei Datenpannen**
- ▲ **EU-DSGVO-Konformität** aller Dokumente/Prozesse

▲ = hoher Aufwand in der Umsetzung zu erwarten

Was kommt auf uns in D zu?

▲ Rechenschaftspflicht (Accountability)

- **Richtlinien/Regeln** zum Datenschutz und zur IT-Sicherheit müssen **vorhanden** sein
- Die **kontinuierliche Anwendung** und Einhaltung dieser Richtlinien/Regeln muss durch Dokumentation/Protokollierung **nachgewiesen** werden.
  Jede betroffene Fachabteilung ist verantwortlich, geeignete Nachweise zu führen. - DSB berät.
- Die **Nachweise** müssen zyklisch geprüft/**auditiert** werden:
  durch FüK / IR / DSB / Zertifizierung
- Die **Richtlinien/Regeln** müssen regelmäßig **überprüft und aktualisiert** werden
  -> **PDCA-Zyklus/KVP** für Datenschutz- und IT-Sicherheitsmaßnahmen wird gesetzliche Pflicht.

Was kommt auf uns in D zu?

▲ Sperr- / Löschpflicht + „Right to be forgotten“

- pbDaten müssen **gelöscht/vernichtet** werden, sobald sie für die Erfüllung des ursprünglichen Zwecks der Speicherung und Verarbeitung n

WIE:

- **Anforderung an SW-Hersteller konsistente Funktionen zur Sperrung/Löschung pbDaten zu implementieren**
- **erneute Prüfung aller eigen erstellten Software auf Implementation von Sperr-/Löschroutinen**
- **konsequente Anwendung der Sperr- und Löschroutinen**

- Is
  V
  erforderlich, müssen sie für den regulären Zugriff **gesperrt/archiviert** werden (durch starke Einschränkung der Zugriffsberechtigungen, DV-technisch, räumlich, etc.).

Was kommt auf uns in D zu?

Informationspflicht (ggü. Mitarbeitern, Kunden/Geschäftspartnern) bei Erhebung pbDaten - Inhalt:

- Name der PxC-Gesellschaft
- Name/Kontaktdaten des DSB
- Zwecke der Verarbeitung
- Rechtsgrundlage der Verarbeitung
- Kategorien der Daten, die verarbeitet werden
- Nennung der „berechtigten Interessen"

- **Speicherdauer der Daten (Löschfrist!)**
- Recht auf Auskunft
- Recht auf Berichtigung, Sperrung, Löschung
- Recht auf Widerspruch
- Recht auf Datenübertragbarkeit
- Recht auf Widerruf seiner Einwilligung

vorläufiges WIE:

Ablage von Informationsblättern zum Download:

- **im Intranet (Mitarbeiter)**
- **im Internet (Kunden/Geschäftspartner/Sonstige)**
- **z. T. kontextbezogen, z. B. bei Web-Eingabemasken**

Was kommt auf uns in D zu?

Auskunftspflicht (+ Datenübertragbarkeit)

- Betroffene (Mitarbeiter, Kunden-/Lieferantenansprechpartner) haben das Recht Auskunft über ihre bei uns gespeicherten/verarbeiteten Daten zu bekommen

- Recht auf Datenübertragbarkeit
  (pbDaten, die eine Person uns zur Verfügung gestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format dieser Person zur Verfügung zu stellen)
  -> spielt für Phoenix Contact faktisch keine Rolle

WIE:

keine Änderung – erfolgt individuell auf Anfrage

Was kommt auf uns in D zu?

IT-Sicherheit (auf Basis Risikoanalyse mit Fokus Betroffener)

- IT-Sicherheitskonzepte müssen nun (auch) auf Basis einer **Risikoanalyse mit Fokus auf die betroffenen Personen** erstellt/angepasst werden
  (Risiko für die *Rechte und Freiheiten* der betroffenen Personen)

WIE:

Durchsicht und Anpassung vorhandener Risikoanalysen des ITSM (Ergänzung und Bewertung spezifischer Risiken aus Sicht der Betroffenen)

Was kommt auf uns in D zu?

Datenschutz-Folgenabschätzungen (+ Risikoanalyse)

vorläufiges WIE:

- **Orientierung an Leitfäden, wie:**
- **Überarbeitung/ Ergänzung der vorhandenen Vorabkontrolle**

( )* = gesetzliche Pflicht, daher möglicherweise Entfall

Was kommt auf uns in D zu?

Meldepflicht bei Datenpannen

WIE:

- keine wesentl. Änderung – Vorgehen ist identisch
- Anpassung des internen Leitfadens
- verstärkte Sensibilisierung der Fachabteilungen im Bezug auf Fälle und Fristen

PHOENIX CONTACT | Meldepflicht eines Datenschutzvorfalls / einer Datenpanne gemäß §42a Bundesdatenschutzgesetz (BDSG) | Januar 2015

Notfallhandbuch

für den Fall eines Datenschutzvorfalls/einer Datenpanne

Hintergrund/Motivation

Das Bundesdatenschutzgesetz (BDSG) sieht im Falle einer unrechtmäßigen Kenntnisnahme bestimmter personenbezogener Daten durch Dritte (z. B. durch Datendiebstahl, Datenverlust, irrtümliche Übermittlung, etc.) eine Meldepflicht vor. Diese Meldepflicht ist sowohl gegenüber der zuständigen Datenschutzbehörde als auch gegenüber den Personen, deren Daten betroffen sind wahrzunehmen und hat von der verantwortlichen Stelle (Phoenix Contact Gesellschaft) zu erfolgen, die für die jeweiligen Daten inhaltlich verantwortlich ist.

Dieser Meldepflicht ist **unverzüglich** (ohne schuldhaftes Zögern) nachzukommen. Was als unverzüglich angesehen wird, bemisst sich an den Umständen des Einzelfalles. Die Meldefrist zählt ab der Kenntnisnahme der Datenpanne durch die verantwortliche Stelle und dient dieser zur Ermittlung des Sachverhaltes und der Prüfung der Voraussetzungen einer Meldepflicht. **Sie sollte zwei Wochen nicht übersteigen!**

Wird dieser Meldepflicht nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig nachgekommen, droht ein Bußgeld von bis zu 300.000 Euro.
(Rechtliche Grundlage: § 42a BDSG i.V.m. § 43 Abs. 2 S. 1 Nr. 7 BDSG)

Dieses Notfallhandbuch dient dazu, den Bearbeitern dieser Meldung (verantwortliche Abteilung, Datenschutzbeauftragter, ggf. Geschäftsführung) an komprimierter Stelle Instrumente an die Hand zu geben, dieser Meldepflicht fristgerecht nachzukommen.

Ersteller:
Helmut Karnath, Datenschutzbeauftragter
Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, 32825 Blomberg

Stand: Januar 2015

PHOENIX CONTACT INSPIRING INNOVATIONS

Was kommt auf uns in D zu?

▲ EU-DSGVO-Konformität herstellen

Überarbeitung diverser DS-Dokumente/Richtlinien/Verträge

- Interne Richtlinien / Formulare
- Verfahrensbeschreibungen („Verzeichnis der Verarbeitungstätigkeiten“)
- Beschreibung der TOMs
- (Muster-)Verträge (ADVn, Datenschutzrahmenvertrag)
- Datenschutzerklärungen (Web, Apps, etc.)
- Schulungsunterlagen Folien, Handouts, eLearnings
- Betriebsvereinbarungen
- …

Was kommt auf uns in D zu?

▲ EU-DSGVO-Konformität (Dokumente)

lfd. Nr.	Bezeichnung des Dokuments / der Dokumente	ID des Dokuments (z. B. IMS-Nr.)	Dokumententyp
1	Verpflichtungserklärung der Mitarbeiter auf das Datengeheimnis nach §5 BDSG incl. der Merkblätter "Datenschutz" und "Informationssicherheit"	FS A-7-0277	Formular
2	Verpflichtungserklärung der Mitarbeiter der IO auf das Telekomm… Fernmelde…	—	Dokument
3	Verpflichtu… auf das Br…		Richtlinie Dokument Präsentation
4	Datenschu…		Präsentation
5	Meldung ü… (Kameras)		Handbuch Orientierungshilfe
6	Prozess Verarbeitu… Lieferanter…		Formular
7	Datenschu…		
8	Musterverträge zur Auftragsdatenverarbeitung incl. Anlage 1-4		
9	Auftragsdatenverarbeitung – Kontrolle des Auftragnehmers (Fragebogen)		
10	ADV-Verträge mit Dienstleistern		
11	Datenschutzverpflichtung(serklärung) für Auftragnehmer		
12	Prozess Erstellung einer Verfahrensbeschreibung gem. Bundesdatenschutzgesetz		
13	Beschreibung der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten (gemäß §§ 4e, 4g BDSG) (Formular Verfahrensbeschreibung)	FS A-7-0277	Formular
14	Verfahrensbeschreibungen	—	Dokument
	gemäß §42a BDSG (mit weiteren Dokumenten)		
22	Notfallhandbuch Datenschutz Auskunftsverlangen nach § 34 BDSG	—	Leitfaden
23	Datenschutzanforderungen bei Softwareerstellung und Softwareauswahl	—	Leitfaden
24	Anforderungen an einen datenschutz- und rechtskonformen Webauftritt	—	Orientierungshilfe
25	Anforderungen an eine datenschutz- und rechtskonforme App	—	Orientierungshilfe
26	Anforderungen an eine datenschutz- und rechtskonformen Newsletterversand	—	Orientierungshilfe

WIE:

Durchlesen und anpassen der Dokumente/Richtlinien/Formulare

Was kommt auf uns in D zu?

▲ EU-DSGVO-Konformität (Verfahrensbeschreibungen)

- Anpassung der Verfahrensbeschreibungen
- Datenschutz-Folgenabschätzung

WIE:

- **Durchlesen und anpassen der Verfahrensbeschreibungen**
  (Rechtsgrundlage und sonst. Bezüge auf das BDSG)
- **Überarbeitung der Vorabkontrolle hin zur Datenschutz-Folgenabschätzung (wenn erforderlich)**

Was kommt auf uns in D zu?

▲ EU-DSGVO-Konformität (ADV-Verträge)

- Phoenix Contact ADV-Mustervertrag anpassen (**Guidance-Dokumente?**)

- Prüfung, welche abgeschlossenen ADV-Verträge auf Basis unseres Vertragsmusters oder auf Basis eines Vertragsmusters des AN erstellt wurden.

geplantes WIE:

- **ab sofort möglichst Hybrid-Verträge (BDSG/DSGVO) abschließen**
- **bis 25.05.2018 für Altverträge Ergänzungsvereinbarungen (2-3-Seiter) abschließen**
- **ab 25.05.2018 neue Verträge ausschließlich nach DSGVO**

Was kommt auf uns in D zu?

▲ EU-DSGVO-Konformität (Betriebsvereinbarungen)

- Prüfung wesentlicher (K)BVn auf DSGVO-Konformität
  - EDV Rahmen-Konzernbetriebsvereinbarung
  - KBV Videoüberwachung
  - etc.

vorläufiges WIE:

- **Abschluss einer Rahmen-KBV/BV zur EU-DSGVO**
- **Erforderlichenfalls Anpassung einzelner, wesentlicher (K)BVn**

Fazit

- EU-DSGVO spielt für Phoenix Contact natürlich eine Rolle
- Die Umsetzung generiert unternehmensweit erhebliche Aufwände
- Der Zeitdruck ist enorm, insbes. auch im Hinblick auf BDSGneu
- WAS getan werden muss ist (inzwischen) relativ klar
- Das größte Problem (momentan) ist das Fehlen von Guidance-Dokumenten für das WIE:
  - konkrete, praxisorientierte Orientierungshilfen
  - Vorlagen, Musterverträge, Musterformulare, etc.
- Mein Eindruck: Die Unsicherheit bei DS-Behörden, DS-Organisationen, Geschäftspartnern, ist noch groß

trotzdem: JA, wir schaffen das! ☺