Dokumentation
Weiterbildung
IT-Systeme

CSI – Computer System GmbH Ilmenau

Unternehmen

CSI ist seit 1990 Dienstleister für Technische Dokumentation, Weiterbildung und IT-Systeme. Erfahrene und kompetente Technische Redakteure und Illustratoren sowie Fachdozenten und Systemingenieure gewährleisten an den Standorten in Ilmenau, Gera und Gotha eine umfassende Betreuung und zuverlässige Umsetzung von Kundenprojekten in hoher Qualität.

Geschäftsbereiche

Technische Dokumentation:

- Erstellung haftungssicherer und normenkonformer Gebrauchsanleitungen von der Konzeption und Gestaltung bis zur Übersetzung der fertigen Anleitung
- Beratung in allen Fragen der Produktdokumentation und CE-Konformität

Weiterbildung:

- bedarfsgerechte Qualifizierung
- Hersteller-Zertifizierungen, Workshops
- Inhouse Seminare und projektbegleitendes Coaching

IT-Systeme:

- Konzeption und Implementierung von Netzwerkinfrastrukturen und Sicherheitslösungen
- Unterweisung und Wartung der IT-Architektur online und vor Ort

ISO 9001 AZAV

zertifiziertes Managementsystem nach DIN EN ISO 9001
Trägerzulassung nach AZAV

Dokumentation
Weiterbildung
IT-Systeme

5 Monate DSGVO

wo "stehen" meine Daten?

Verordnung (EU) 2016/679 des Europäischen Parlaments
und des Rates

Computer System GmbH

cs-ilmenau.de

Dokumentation
Weiterbildung
IT-Systeme

Heiko Langenhan

Geschäftsführer
Leiter IT- Systeme – externer Datenschutzbeauftragter

Mehr als 4 Jahre Erfahrung im Datenschutz
Consultant für IT-Infrastruktur-Lösungen

IT-Systeme

IT-Infrastruktur-Lösungen
Dienstleistung IT-Infrastruktur – Administration / Service & Support
externer Datenschutzbeauftragter
Analyse & Consulting IT-Security (VdS 3473)

Computer System GmbH Ilmenau
Amtsstraße 3
98693 Ilmenau
Tel.: +49 3677 6480-40
Fax: +49 3677 6480-55
h.langenhan@cs-ilmenau.de
www.cs-ilmenau.de
www.csi-technik.de

Warum ist Datenschutz notwendig?

Datenschutz ist notwendig zur freien Entfaltung der Persönlichkeit jedes Menschen

„Grundrecht auf informationelle Selbstbestimmung“
Schutz der Privatsphäre: Kenntnis darüber, welche Daten wo gespeichert sind. (Volkszählungsurteil vom 15.12.1983)

„Grundrecht auf digitale Intimsphäre“
Schutz der Daten in IT-Systemen sowie deren Vertraulichkeit und Integrität.

BUNDES-
VERFASSUNGS-
GERICHT

Die DSGVO schreibt vor…

Wann darf rechtmäßig verarbeitet werden?

Der Grundsatz gilt weiter: **Verbot mit Erlaubnisvorbehalt**

Artikel 6 Abs. 1:

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die Person hat ihre Einwilligung zu der Verarbeitung … für einen oder mehrere bestimmte Zwecke gegeben;
b) die Verarbeitung ist für die Erfüllung eines Vertrags, … die auf Anfrage der betroffenen Person erfolgen;
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt (andere Gestze);
d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, … überwiegen, insbesondere dann, wenn es sich … um ein Kind handelt.

Die DSGVO schreibt vor…

Grundregeln

Rechtsgrundlage:
Immer wenn personenbezogene Daten „angefasst“ werden, muss es dafür eine Rechtsgrundlage oder eine Einwilligung geben.

Daten beim Betroffenen erheben:
Wenn möglich, sind die Daten immer direkt beim Betroffenen zu erheben. Wenn nicht, ist er i. d. R. zumindest darüber zu informieren
(informationelle Selbstbestimmung).

Auskunftsrechte:
Der Betroffene muss jederzeit Kenntnis haben, dass und welche Daten über ihn gespeichert werden. Betroffener darf Auskunft verlangen! (Auskunftsrecht)
(Artikel 13 / 14 / 15 EU-DSGVO)

…

Die DSGVO schreibt vor…

…

Zweckbestimmung:
Erhobene Daten dürfen ausschließlich nur für den ursprünglich Zweck, für den sie erhoben wurden, verwendet werden.

(Artikel 5 EU-DSGVO Grundsätze für die Verarbeitung personenbezogener Daten)

Datensparsamkeit:
So wenig Daten wie nötig dürfen erhoben, verarbeitet und genutzt werden.

Berichtigung:
Fehler oder falsche personenbezogene Daten müssen berichtigt werden.

(Artikel 16 EU-DSGVO Berichtigung).

Schutz durch technische und organisatorische Maßnahmen:
Daten müssen vor Missbrauch, Beschädigung oder Verlust geschützt werden.

(Artikel 32 EU-DSGVO Sicherheit der Verarbeitung).

5 Monate DSGVO

„Es ist leichtfertig zu hoffen, dass nichts passiert“

Ein verantwortungsvollerer neuartiger Umgang mit personenbezogenen Daten finden gefühlt nicht statt, alle sind eigentlich nur genervt.

Ca. 70% der KMUs haben kein Datenschutzmanagement (nur Datenschutz auf der WEB-Site)

Stellen, in den besonders schützenswerte Daten verarbeitet werden sind am unsichersten, da hier der Aufwand zum Schutz wesentlich höher sein muss. (Ärzte, Schulen, Behörden,...)

Die große Frage zur Rechtssicherheit bleibt offen.

Die Behörde (TLfDI) sind auch nicht allwissend und können keine Rechtssicherheit bieten.

Die Behörden überprüfen nur auf Anzeigen und werden nicht selbständig tätig.

Dokumentation Weiterbildung IT-Systeme

5 Monate DSGVO

Die Welle von DSGVO-Abmahnungen blieb aus, aber der Handlungsbedarf bleibt!

Rechtsunsicherheit herrscht hier bezüglich der Anwendbarkeit des Gesetzes gegen den unlauteren Wettbewerb (UWG), welches einschlägige Datenschutzvorschrift als Marktverhaltensregelung i.S.v. § 3a UWG einordnet und somit die Grundlage für eine Abmahnung bietet.

DSGVO selbst sieht die Möglichkeit einer Abmahnung bei datenschutzrechtlichen Verstößen nicht vor.

Mit einem Beschluss des LG Würzburg vom 13.09.2018 gibt es eine erste gerichtliche Entscheidung über die wettbewerbsrechtliche Abmahnfähigkeit von DSGVO-Verstößen.

- eine lediglich 7-zeilige Datenschutzerklärung im Impressum
- fehlende Informationspflichten aus Art. 13 DSGVO
- Verstöße gegen das Wettbewerbsrecht gemäß § 3 a) UWG

Dokumentation Weiterbildung IT-Systeme

5 Monate DSGVO

telefonische Kaltakquise im B2B nach DSGVO verboten?

Relevant sind und bleiben die Vorschriften des unlauteren Wettbewerbsgesetz (UWG).

Risiko ist die Fehleinschätzung einer mutmaßlichen Einwilligung.

Nach DSGVO Art. 6 Abs. 1 muss stets eine Abwägung (argumentativ mit Leben gefüllt) des berechtigten Interesses vorgenommen werden. (Eigene Interessen müssen überwiegen!)

Umsetzung der Informationspflichten ist mit der Übermittelung im „zeitlichen Zusammenhang“ - mit nachfolgendem Brief oder nachfolgender E-Mail möglich.

Liegt eine Einwilligung vor ist die Kaltakquise unproblematisch.

5 Monate DSGVO

Verantwortliche Stelle und Auftragsverarbeiter
Wie ist die Haftung untereinander?

Verantwortliche Stelle und Auftragsverarbeiter haften als Gesamtschuldner für einen durch die Datenverarbeitung entstandenen Schaden, Art. 82 DSGVO.

Jeder haftet auf die volle Summe!

Im Innenverhältnis kann die Haftungsverteilung untereinander regelmäßig selbst ausgestaltet werden.

- Die verantwortliche Stelle hat die Leitungsmacht über den Datenverarbeitungsprozess und haftet bei dessen Nichteinhaltung
- Der Auftragsverarbeiter haftet, wenn er Weisungen der verantwortliche Stelle missachtet oder seinen gesetzlichen Pflichten nicht nachkommt.

Dokumentation Weiterbildung IT-Systeme

5 Monate DSGVO

Selbstbelastungsfreiheit vs. Mitwirkungspflicht beim Datenschutzverstoß

Der Grundsatz der Selbstbelastungsfreiheit - das Prinzip, dass niemand verpflichtet ist, an seiner eigenen Verurteilung mitzuwirken, ist ein Grundsatz vom Verfassungsrang.

Melde- und Mitwirkungspflichten - die Datenschutz-Grundverordnung enthält mit Art. 33 eine Vorschrift, die verantwortliche Stellen dazu zwingt, ggf. eigene Verstöße gegen datenschutzrechtliche Vorschriften der zuständigen Aufsichtsbehörde zu melden.

Bei Verstoß gegen die Meldepflicht droht ein Geldbuße von bis zu EUR 10 000 000 oder 2 % des weltweiten Jahresumsatzes.

Gemäß § 43 Abs. 4 BDSG darf eine Meldung in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen nur mit Zustimmung des Meldepflichtigen verwendet werden.

Bei Nichteinhaltung der DSGVO/BDSG droht ein Geldbuße von bis zu EUR 10 000 000 oder 2 % des weltweiten Jahresumsatzes.

Dokumentation Weiterbildung IT-Systeme

5 Monate DSGVO

Datenschutz im Sportverein
Erhebung von Leistungsdaten

Die Erhebung von Leistungsdaten lassen mittelbare Rückschlüsse auf den Gesundheitszustand des Sportlers zu. Diese Daten sind somit zu sogenannten „sensiblen Daten“ im Sinne des Art. 9 DSGVO zu zählen.

Zweck der Verarbeitung muss definiert und eingehalten werden.

Weitergabe (Veröffentlichung) muss genau organisiert werden (Einwilligung).
(Wer kann die Daten analysieren, vergleichen und anwenden – Profiling)

Eine Datenschutz-Folgenabschätzung gem. Art. 35 Abs. 3 DSGVO ist erforderlich.

Ein Datenschutzbeauftragter ist zu benennen.

Dokumentation Weiterbildung IT-Systeme

Wo liegen meine Daten

Amazon, Facebook, WhatsApp, Google,...

„Globale Player“ stehen nun ständig auf dem Prüfstand!

Beispiele:

Google Signals – Personalisierte Zugriffe eines Nutzer mit verschiedenen Geräten erkennen – „Google Signals“–Nutzer erhalten bei diesem Dienst nur die Statistik ohne personenbezogene Daten. Google jedoch kann Personen zuordnen, da sie sich bei Google angemeldet haben. (Aktuell kein Einwilligungsverfahren verfügbar, nur Widerspruchsmöglichkeit)

Facebook - nutzt Nummern aus Zwei-Faktor-Authentifizierung für Werbung

Facebook - Hacker hatten Zugriff auf 50 Millionen Nutzerkonten - eine Sicherheitslücke bei der „View-As“ Funktion von Facebook.
„Stimmen werden laut, die in diesem Fall ein erstes Bußgeld nach der DSGVO sehen.“
Unklar ist, ob ein Sicherheitsvorfall immer auch bußgeldrelevant im Sinne der DSGVO ist.

Dokumentation Weiterbildung IT-Systeme

Wo liegen meine Daten

Amazon, Facebook, WhatsApp, Google,...

Was bedeutet der Vorfall bei Facebook für kleinere Unternehmen?

Datensicherheit wird in deutschen KMUs mit großen Abstrichen umgesetzt.

Ausschlaggebend ist dafür ein wenig ausgeprägtes Risikobewusstsein in der Führungsebene.

Datensicherheit kostet Geld und geht zu Lasten der Nutzerfreundlichkeit.

Oder, getreu nach dem Motto „Wir haben keine wichtigen Daten“ oder „Für uns interessiert sich eh niemand“.

Einige Entscheidungen gehen dann gegen die Datensicherheit und somit auch gegen den Datenschutz.

Diese sind vor dem Hintergrund der DSGVO und der Zunahme von Cyber-Attacken allerdings fahrlässig!!!

KMUs müssen zukünftig Datensicherheit mehr in den Vordergrund stellen und die Kosten dafür einkalkulieren. (Nutzung neuer Cloud-Dienste, Datenanalyse-Software Tracking-Methoden,...)

Bei Feststellung eines Verstoßes müsste die Aufsichtsbehörde ein Bußgeld verhängen.

Chancen und Risiken

Die Umsetzung und Einhaltung ist nicht schwer

Interner / externe Datenschutzbeauftragter

5-15 Tage zur Erstellung eines Datenschutzmanagements

Beratung ist förderfähig mit ESF-Mittel (max. 20 Werktage bis je 800,00 € zu 50%)

Die Behörden veröffentlichen regelmäßige immer mehr Handlungsempfehlungen:

In Thüringen: https://www.tlfdi.de/tlfdi/gesetze/europaeische-dsgvo/
Interessant ist auch Bayern: https://www.datenschutz-bayern.de/info/

Dokumentation Weiterbildung IT-Systeme

Chancen und Risiken

Die Umsetzung und Einhaltung ist nicht schwer

Kurzpapiere der Datenschutzkonferenz – DSK

… erste Orientierung insbesondere für den nicht-öffentlichen Bereich….nach Auffassung der DSK die DS-GVO … angewendet werden sollte. … unter dem Vorbehalt zukünftiger … abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Kurzpapier Nr. 1: Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO
Kurzpapier Nr. 3: Verarbeitung personenbezogener Daten für Werbung
Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
Kurzpapier Nr. 6: Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO
Kurzpapier Nr. 8: Maßnahmenplan „DS-GVO“ für Unternehmen
Kurzpapier Nr. 10: Informationspflichten bei Dritt- und Direkterhebung
Kurzpapier Nr. 11: Recht auf Löschung / „Recht auf Vergessenwerden“
Kurzpapier Nr. 12: Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern
Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DS-GVO
Kurzpapier Nr. 14: Beschäftigtendatenschutz
Kurzpapier Nr. 17: Besondere Kategorien personenbezogener Daten
Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen

Dokumentation Weiterbildung IT-Systeme

Chancen und Risiken

Compliance für Ihr Unternehmen – Datenschutz und IT

Minimieren des steigenden Risikos

- Unternehmerisches Risiko
- Technisches Risiko

Vertrauen gegenüber Ihrer Kunden

Vertrauen gegenüber Geschäftspartnern (Lieferanten, Banken, Verbänden,..)

ToDo:

1. Datenschutzmanagement
2. IT-Sicherheitskonzept
3. IT- Notfallplan
4. Cyber-Versicherung

Fazit

Datenschutz ist und bleibt Chefsache

Stärkung und Präzisierung der Rechte der betroffenen Personen und deren Aufklärung führt zu mehr Risiken für KMUs.

Datensicherheit wird immer wichtiger - es kostet Zeit und Geld!

Es ist leichtfertig **und fahrlässig** zu hoffen, dass nichts passiert!

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?