KRZ.AKTUELL

SONDERAUSGABE Mai 2018

SÜDWESTDEUTSCHLAND

Nach zwei Jahren Übergangsfrist tritt am 25.5.2018 die EU-DSGVO in Kraft, die Datenschutzgesetze der evangelischen und katholischen Kirche bereits am 24.5.2018. Ein großer Teil der Regelungen der DSGVO ist bereits bekannt, einige Verpflichtungen werden jedoch erweitert oder sind neu.

Mit dieser Sonderausgabe der KRZ.AKTUELL möchten wir Ihnen die wichtigsten Grundbegriffe und Grundprinzipien näher erläutern und Ihnen darüber hinaus mitteilen, wie das KRZ-SWD mit diesen neuen Vorgaben umgeht bzw. in welcher Form diese umgesetzt wurden.

Europäische Datenschutz-Grundverordnung

Personenbezogene Daten, d. h. Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen oder dieser zugeordnet werden können (Name, Adresse, Fotos etc.) oder auch **besondere Kategorien personenbezogener Daten** (rassische und ethnische Herkunft, politische und weltanschauliche Überzeugungen und Gesundheitsdaten sowie (neu!) biometrische Daten), dürfen weiterhin nur verarbeitet werden, wenn hierfür eine Erlaubnis besteht. Die Verarbeitung muss transparent sein, d. h. die betroffene Person muss informiert werden, wenn Daten über sie erhoben und verarbeitet werden.

Die Speicherung, Nutzung und Verarbeitung von personenbezogenen Daten **ist** stets in Abhängigkeit zu einem bestimmten Zweck zu setzen, sowie auf das für die Zwecke der Verarbeitung notwendige Maß zu beschränken („Datenminimierung“). Werden personenbezogene Daten nicht mehr benötigt, sind diese unverzüglich zu löschen und die Empfänger zu informieren („Recht auf Vergessenwerden“).

Es besteht eine grundsätzliche **Rechenschaftspflicht**, als Konsequenz daraus müssen datenverarbeitende Organisationen ein Datenschutzmanagement vorweisen. Verantwortliche müssen angemessene organisatorische und technische Schutzmaßnahmen treffen, um die **Datensicherheit** zu gewährleisten.

Bei Datenpannen muss die Aufsichtsbehörde innerhalb von 72 Stunden benachrichtigt werden. Die zur Verarbeitung personenbezogener Daten autorisierten Personen sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht.

Hersteller sind verpflichtet, Produkte datenschutzfreundlich zu gestalten (Privacy-by-Design/Privacy-by-Default).

Jeglicher Verstoß gegen die Europäische Datenschutz-Grundverordnung wird mit einem Bußgeld geahndet, welches bei 2 % bzw. 4 % des konzernweiten Jahresumsatzes oder 10 bzw. 20 Millionen Euro liegt. Im kirchlichen Bereich reicht die Bußgeldspanne bis 500.000 Euro.

ISO 27001

Die internationale Norm ISO 27001 beinhaltet Anforderungen und Maßnahmen für die Beurteilung und Behandlung von Informationsrisiken. Sie beschreibt die Anforderungen für das Einrichten, Realisieren, Betreiben und Optimieren eines dokumentierten Informationssicherheits-Managementsystems.
Mit der Zertifizierung erbringt die Organisation den dokumentierten Nachweis, dass die Anforderungen der Informationssicherheit eingehalten und die Maßnahmen zum Schutz von Daten umgesetzt sind. Kunden und Geschäftspartner erhalten dank der Zertifizierung einen vertrauenswürdigen Beleg dafür, dass eine geprüfte, sehr gute IT-Sicherheit gewährleistet werden kann.

Sicherheit in stürmischen Zeiten…

Das KRZ-SWD hat sich früh mit der Thematik auseinandergesetzt und die Vorgaben der EU-DSGVO sowie ISO 27001 wie folgt umgesetzt:

- Im Herbst 2017 wurde unser KRZ.Dual-Rechenzentrum errichtet, welches seit Anfang 2018 als „full managed service“ (24x7) im produktiven Betrieb ist. Damit ist die sichere Verarbeitung und Haltung der Daten an zwei voneinander getrennten Standorten gewährleistet.
- Das KRZ-SWD hat die ISO/IEC 27001:2013-Zertifizierung erfolgreich bestanden. Vertraulichkeit, Verfügbarkeit und Integrität im Umgang mit Kunden- und KRZ-Daten wurden im März 2018 durch eine unabhängige Stelle im Informationsmanagementsystem „ISMS“ geprüft und bescheinigt. Sowohl die technischen als auch organisatorischen Maßnahmen („TOM“) entsprechen dem Stand der Technik.
- Neben dem Informationsmanagementsystem „ISMS“ etabliert das KRZ-SWD ein Datenschutzmanagementsystem „DSMS“, um dem Erfordernis der Rechenschaftspflicht, der Einhaltung von Meldepflichten sowie der kontinuierlichen Überprüfung und Verbesserung Rechnung zu tragen.
- Mit unserer extern bestellten Datenschutzbeauftragten finden regelmäßige Besprechungen statt. Alle Mitarbeiter/innen des KRZ-SWD sind dem Datenschutz verpflichtet, werden regelmäßig auf Datenschutz und Informationssicherheit geschult und haben im April 2018 eine Schulung zur EU-DSGVO erhalten.
- Die Verträge mit unseren Kunden wurden proaktiv bearbeitet und an die Anforderungen des EKD-DSG sowie KDG angepasst. Unsere Beschreibung der internen Geschäftsprozesse wurde den Datenschutzgesetzen der evangelischen und katholischen Kirche angeglichen.

KRZ-SWD … wir kümmern uns – versprochen!

Die Themen Datenschutz, Datensicherheit und Digitale Transformation behandeln wir auch auf unserem **KRZ.IT-Sicherheitstag** am 9. November 2018.


ZERTIFIKAT

ISO/IEC 27001:2013

IMPRESSUM

Stiftung Kirchliches Rechenzentrum Südwestdeutschland
Junkersring 10
76344 Eggenstein-Leopoldshafen
redaktion@krz-swd.de
www.krz-swd.de

Verantwortlich für den Inhalt:
Jochen Gamber, KRZ-SWD

Redaktion: Dr. Reiner Weick, Christina Bonset, KRZ-SWD

Gestaltung und Produktion:
Stober GmbH, Eggenstein

Bildnachweis:
©Jan Engel - Fotolia.com