FAIR COMPUTER SYSTEMS GMBH

DSGVO DATENBLATT

DSGVO-Compliance für die IT-Infrastruktur
Seit dem 25.05.2018 gilt die EU-Datenschutz-Grundverordnung (DSGVO).
Diese muss bei allen angewendet werden, die mit personenbezogenen Daten von EU-Bürgern arbeiten.
Die neuen Richtlinien haben auch umfassende Auswirkungen auf die IT-Abteilung. Es gelten strengere Regeln für den Umgang mit entsprechenden Daten und härtere Strafen bei Verstößen.
Dabei ist ein wichtiger Aspekt einer erfolgreichen Gefahrenabwehr im Bereich IT-Sicherheit die Ausarbeitung interner Vorgänge, deren Bewertung und Protokollierung. Es müssen technisch-organisatorische Maßnahmen geschaffen sowie DSGVO-Prinzipien in der IT-Infrastruktur implementiert werden. Doch die Herstellung einer umfassenden und unternehmensweiten DSGVO-Compliance ist ein umfangreiches Verfahren, welches unterschiedliche Komponenten wie Technologie, Leitlinien und organisatorische Faktoren einbeziehen muss.

Welche Lösungsansätze die FCS-Produkte in Bezug auf die DSGVO für die IT-Infrastruktur im Unternehmen bietet, zeigen folgende Beispiele:

	DSGVO-Prinzipien	Fallbeispiel im Unternehmen	Lösungsansatz mit FCS
DSGVO-Compliance	**Compliance von Betriebssystemen**	Das Betriebssystem Windows 10 soll im Unternehmen auf allen Mitarbeiter-PCs ausgerollt werden. Zuvor sollen aber datenschutzkonforme Einstellungen von den IT-Verantwortlichen im Unternehmen definiert werden.	Install.Desk OSIS unterstützt die Installation und Konfiguration von u.a. Server-Betriebssystemen oder Windows 10. Datenschutzkonforme Einstellungen (z.B. Deaktivierung Cortana, Nicht-Senden von Nutzungsstatistiken) und Upgrades können mit OSIS konfiguriert werden.
Anforderungen	**Art. 32, Abs. 1a DSGVO: Verschlüsselung personenbezogener Daten**	Versehentliche Weitergabe von wichtigen Geschäftsdaten und der Verlust oder Diebstahl mobiler Geräte, wie Wechselspeichermedien, Tablets und Smartphones können im Unternehmen Millionenschäden verursachen. Dieses Risiko wollen die IT-Verantwortlichen auf ein Minimum beschränken.	Mit Hilfe von Disc.Secure lassen sich gefährdete Unternehmensdaten (Kundeninformationen, Pläne, Kennzahlen etc.) durch AES-256-Bit-Verschlüsselung in einem sicheren Container auf dem jeweiligen PC, oder auch auf einem Stick, speichern und mit einem Passwort schützen. Den sicheren Transfer mobiler Daten gewährleistet der Hardware-verschlüsselte USB-Stick Storocrypt.
	Art. 32, Abs. 1d DSGVO: Wirksamkeit von Sicherheitsmaßnahmen regelmäßig überprüfen	IT-Verantwortliche im Unternehmen möchten Schwachstellen hervorheben, Risiken verringern und Maßnahmen sinnvoll priorisieren.	Das Schwachstellenmanagement der Softwareverteillösung Install.Desk hilft, kritische Sicherheitslücken in der IT zu erkennen, Risiken mittels CVSS- und CVE-zertifizierter Handlungsempfehlungen zu beseitigen und automatisierte Jobs festzulegen. Im Nachgang kann überprüft werden, ob die identifizierten Schwachstellen erfolgreich beseitigt wurden.
	Art.15 DSGVO: Auskunftsrecht der betroffenen Person	Ein Mitarbeiter im Unternehmen möchte von seinem Administrator Informationen erhalten, welche personenbezogenen Daten von ihm gespeichert sind.	Die in Asset.Desk verwendeten personenbezogenen Daten (z.B. IP-Adressen) können vom Administrator bei Bedarf angezeigt und exportiert werden.
	Art. 25 DSGVO: Privacy by Design/Default	Ein Mitarbeiter möchte nicht, dass seine Energiedaten und Nutzungsdaten von seinem PC protokolliert werden.	Asset.Desk erfasst lediglich Adressdaten, aber keinerlei sonstige personenbezogene Daten, wie z.B. Geschlecht, Gesundheitsdaten, Energiedaten. Nutzungsdaten von Software-Anwendungen können über das Asset.Desk Application Metering zum Zwecke des Lizenzmanagements gesammelt werden. Dessen Einsatz bedarf es aber einer besonderen Genehmigung z.B. des Betriebsrates.

Anforderungen			
	Art. 17 DSGVO: Recht auf Löschung (Recht auf "Vergessenwerden")	Ein Mitarbeiter verlässt das Unternehmen und möchte nicht, dass seine personenbezogenen Daten weiterhin gespeichert bleiben. Personenbezogene Daten in Verträgen und Belegen müssen sich löschen lassen, wenn der betriebliche Zweck nicht mehr gegeben ist und keine gesetzlichen Vorgaben dagegen sprechen.	Der Administrator hat in Asset.Desk, HEINZELMANN ServiceDesk und Security.Desk die Möglichkeit, die gespeicherten personenbezogenen Daten anzuzeigen und diese zu löschen. In Asset.Desk kann z.B. vorgegeben werden, welche Belege (Verträge, Angebote, Bestellungen, Rechnungen etc.) samt der personenbezogenen Daten nach wie vielen Jahren (Standard: 10 Jahre) vom System automatisch gelöscht werden sollen. So wird Asset.Desk der Aufbewahrungspflicht und gleichzeitig dem DSGVO-Löschanspruch gerecht.

Allgemein			
	Art. 5 DSGVO: Richtigkeit	Um die richtigen Maßnahmen zur Verwaltung der Infrastruktur zu treffen, ist der IT-Administrator darauf angewiesen, dass alle Infrastruktur-Daten auf dem neuesten Stand sind.	Mit der IT-Inventarisierung von Asset.Desk können sämtliche Betriebssysteme automatisch gescannt und inventarisiert werden. Darunter: Hard- und Software Scan, Windows-, Linux-, MacOS-Geräte, SNMP-Geräte, Thin Clients, (IGEL), AIX- und Solaris-Server, vCenter- und Cloud-Umgebungen sowie manuelle IT-Erfassung. Damit lässt sich stets ein Abbild der Hardware und installierten Software aufzeigen, welches akkurat und auf dem neusten Stand ist.
	Art. 5 DSGVO: Zweckbindung	Die IT-Verantwortlichen im Unternehmen müssen Kenntnis haben, welche personenbezogenen Daten in ihren eingesetzten Softwareprodukten verarbeitet werden.	Die Zweckbindung der erfassten Daten wird in den zugehörigen Dokumentationen der Software geliefert. Die personenbezogenen Daten, die in den FCS-Produkten verarbeitet werden, sind im Handbuch für jedes Modul charakterisiert und deren Zweckbindung festgehalten.

DSGVO
KONFORM

Viele Unternehmen verfügen nicht über eine aktuelle und vollständige Übersicht, wenn es ihre Netzwerkarchitektur sowie ihrer gesamte Hard- und Software betrifft.
In vielen Fällen unterliegen diese Strukturen täglichen Änderungen und oftmals fehlt die Zeit, die Neuerungen umfassend zu dokumentieren.
Datenschutzbeauftragte können ihren Prüfungspflichten – ob nach BDSG oder DSGVO – deshalb nur schwer nachkommen.
Allerdings kann mit den richtigen Lösungen dieser Zustand behoben werden.

Die FCS-Produkte sind DSGVO-konform!
Zudem berücksichtigt FCS seit Jahren die Vorgaben des Bundesdatenschutzgesetzes (BDSG) und leistet seither einen wichtigen Beitrag für die Datenschutz-Compliance bei seinen Kunden.

FCS Fair Computer Systems GmbH
Ostendstraße 132
90482 Nürnberg
+49 (0) 911 810 881 0

www.fair-computer.de

FAIR COMPUTER SYSTEMS GMBH

2018

Sitz und Registergericht: Nürnberg, HRB-Nr. 16405 | USt-IdNr. DE-211630166