PG1

EU-DSGVO

Inkrafttreten: 24. Mai 2016
Anzuwenden ab: 25. Mai 2018

Ein neues Datenschutz-Zeitalter beginnt….

Folie 1

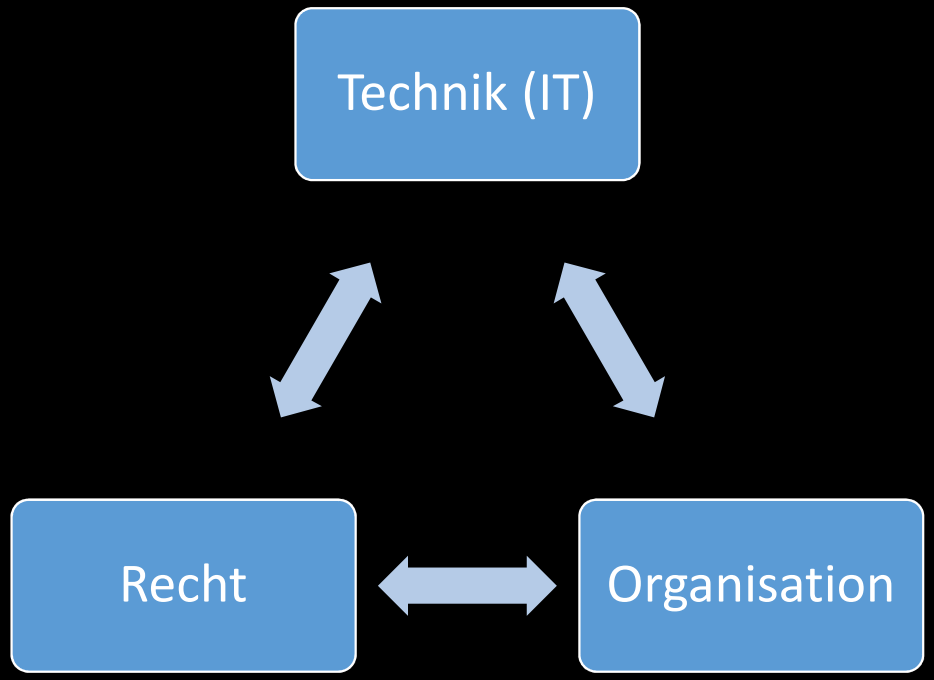
PG1 Praschl Gernot; 12.11.2017

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz von personenbezogenen Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Im noch aktuellen Datenschutzgesetz 2000 sind auch personenbezogene Daten juristischer Personen, also von Unternehmen, Vereinen, Stiftungen etc. geschützt. Dieser Schutz ist in der EU-DSGVO nicht mehr vorgesehen. Zukünftig haben nur noch natürliche Personen Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten.

Sollte die EU-DSGVO nicht ordnungsgemäß umgesetzt werden, drohen Strafen von bis zu EUR 10 Mio. oder 2% Ihres weltweiten Jahresumsatzes bzw. (in einigen Fällen) auch von EUR 20 Mio. oder 4 % Ihres weltweiten Jahresumsatzes. Gemäß der DSGVO sollen die zu verhängenden Strafen „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein (Artikel 83).

EU-DSGVO – Ein reines IT-Thema?



Verzeichnis von Verarbeitungstätigkeiten

Artikel 30 DSGVO

-Kontaktdaten der Verantwortlichen bzw. Mitverantwortlichen

-Zwecke der Verarbeitung (Rechtsgrundlage!), Beschreibung der Kategorien Personen/Daten

-Kategorien von Empfängern (Drittland)

-Wenn möglich, vorhergesehene Fristen für Löschung

-TOMS Artikel 30 DSGVO

-Ersetzt Datenverarbeitungsregister (DVR) Meldung

Verantwortlicher und Auftragsverarbeiter!!

Diverse Vorlagen im Web verfügbar z.B. WKO.

Exel.

Verzeichnis von Verarbeitungstätigkeiten – FORTSETZUNG

Das ist ein Beweismittel!! Behörde!!

Sämtliche Verarbeitungstätigkeiten -> Prozesse!!!

Dokumentationspflicht!!!

Verantwortliche in den Fachabteilungen!!! Neue Rolle!!! Awareness!!!

Verzeichnis muss immer auf neuestem Stand sein!!!

Dieser Prozess endet NIE!!!

Datenschutz Management System

Zentrale Datenbank für die Modellierung und Bewertung der EU-DSGVO-Anforderungen. (Prozesse, Dokumentation, Verantwortliche, Risikoabschätzung, Datenflussdiagramme etc).

Automatisches Berichtswesen - auf Knopfdruck – Verfahrensverzeichnis, Compliance Berichte, Datenschutz-Folgeabschätzungsbericht.

„Noch einige“ EU-DSGVO HIGHLIGHTS

Zustimmungserklärung

Es müssen mehr Voraussetzungen für eine wirksame Zustimmungserklärung erfüllt sein. Sie müssen nun auch einen Nachweis erbringen, dass Sie die Zustimmungserklärung tatsächlich wirksam eingeholt haben.

Auskunftsrecht der Betroffenen

Das Auskunftsrecht der Betroffenen (Artikel 13 und 14 DSGVO) gibt den betroffenen Personen mehr Rechte; die Informationspflichten gegenüber den betroffenen Personen werden ausgeweitet. Sie müssen Ihre Auskunftsverpflichtung innerhalb eines Monats erfüllen (bisher betrug diese Frist acht Wochen).

Daten an Dritte

Sie sind nach der DSGVO verpflichtet, die Empfänger von Daten über Änderungen der Daten zu informieren. Sollten Sie daher Daten über Betroffene an Dritte weitergeben, sind Sie in Zukunft verpflichtet, Löschungen bzw. Richtigstellungen an die Übermittlungsempfänger weiterzugeben.

Daten von Dritten

Recht auf „Datenübertragbarkeit“.

Der Betroffene hat ein Recht auf „Datenübertragbarkeit“. Sie müssen die technischen Voraussetzungen schaffen (maschinenlesbares Format), dass der Betroffene die von Ihnen verarbeiteten Daten zu einem Dritten mitnehmen kann.

Verzeichnis von Verarbeitungstätigkeiten

Sie müssen ein Verzeichnis von Verarbeitungstätigkeiten erstellen. Dafür müssen Sie keine Meldung mehr an das Datenverarbeitungsregister erstatten. Diese „Selbstverpflichtung“ kann von der Datenschutzbehörde jederzeit überprüft werden. Stichwort -> Datenschutz Management System

Recht auf Löschung – Recht auf Vergessen

Betroffene Person hat das Recht auf unverzügliche Löschung der Daten, wenn

-Für die Zwecke nicht mehr notwendig

-Einwilligung widerrufen und keine andere Rechtsgrundlage etc.

TOMS

Angemessene technische und organisatorische Maßnahmen zur wirksamen Umsetzung der DSGVO und zwar unter der Berücksichtigung (Art 25)

-des Stand der Technik und Implementierungskosten

-der Art des Umfangs, der Umstände, des Zweck der Verarbeitung

-der Eintrittswahrscheinlichkeit und schwere der Risiken

-z.B. Pseudoanonymisierung , Datenminimierung

-Privacy by design, Privacy by default

Stand der Technik –

Firewalls, Policy, Netzwerk, Patches, Backup Restore Tests, Verschlüsselung, Audits, Zertifizierungen etc….. Meistens Bewertung durch SV.

Meldung an die Aufsichtsbehörde bei Verletzung - DATA BREACH

Sie müssen (nachweislich) einen Prozess eingerichtet haben, der es Ihnen ermöglicht, die Aufsichtsbehörde binnen 72 Stunden zu informieren, sollte der Schutz von personenbezogenen Daten verletzt worden sein. Gleichzeitig trifft Sie auch die Verpflichtung, einen Prozess zu implementieren, dass Sie die jeweilige betroffene Person über die Verletzung informieren können.

Beschreibung der Folgen!!! Folgeabschätzung!!!

Wenn hohes Risiko für Rechte und Freiheiten

z.B. Nicht notwendig wenn

Geeignete TOMS umgesetzt wurden.

Es ist eine echte Chance!

<u>Möglichkeit, Prozesse, Organisationsabläufe und IT-Anwendungen im Unternehmen proaktiv zu gestalten (Standards)</u>

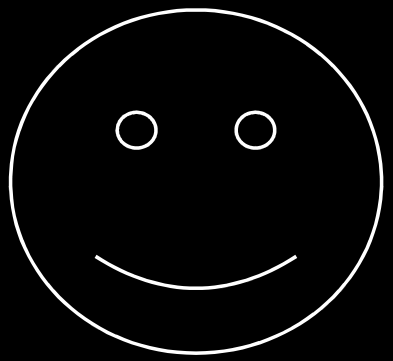
Transparenz schaffen

Vertrauen in das Unternehmen durch öffentliche Bekenntnis zu Datenschutz (Zertifizierungen).

Qualitätsanspruch und Qualitätsniveau

Sicherung der Marktposition

Synergien, Optimierung, Kostenersparnis



Danke für die Aufmerksamkeit!