Neue Datenschutzverordnung (DSGVO/GDPR) und ihre Auswirkungen auf die Sicherheitsbranche und CH-Unternehmen

Wolfgang Sidler

Stv. des Datenschutzbeauftragten des Kantons Luzern, Geschäftsinhaber SIDLER Information Security GmbH, Hünenberg

SES
Verband Schweizerischer Errichter von Sicherheitsanlagen
Association Suisse des Constructeurs de Systèmes de Sécurité
Associazione Svizzera dei Costruttori di Sistemi di Sicurezza

Agenda

- Neue Erkenntnisse 180 Tage nach Einführung (25.5.2018)
- Neue Aspekte für den SiBe oder DSB im Unternehmen
- Wer haftet für Datenschutzverstösse beim Einsatz von Video-Security, Zutrittskontrolle, Einbruchmeldetechnik?
- Tipps und Tricks zur sicheren Umsetzung und Einhaltung der DSGVO – Erfahrungen aus der Praxis
- Herausforderungen Cloud, IoT, Big Data und KI

Neue Erkenntnisse - 180 Tage nach Einführung

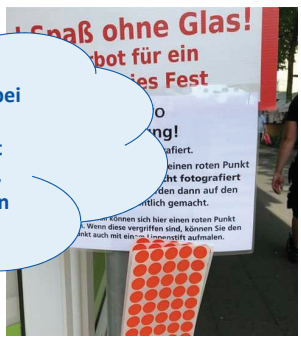
Was wurde aus dem DSGVO-Hype?

- Manche Befürchtungen stellten sich als übertrieben heraus
  → es wurde ruhi
- Wir warten auf d

Fazit:

- Setzen Sie d
  Nicht für die D
  Unternehmen. Bereit
  auf das neue Schweizerisch
  (DSG) vor (2020)!

Die DSGVO ist ein wertvolles Werkzeug bei der Umsetzung Ihrer Digitalisierungs-Strategie. Denn starker Datenschutz ist wichtiger denn je, schafft Transparenz, Vertrauen zum Kunden und sorgt für ein seriöses Auftreten.



Neue Erkenntnisse - 180 Tage nach Einführung

Das Gute an DSGVO

- Es fand eine Sensibilisierung im Bereich des **«Datenschutzes»** statt. Denn mit der Digitalisierung und de… es jetzt … Dat… mach… Ihnen … anzugehen.
- Ziel ist, unsere Privatsphäre zu schützen – es geht um den **«Persönlichkeitsschutz»** und dies speziell, wenn es um unsere «besonders schützenswerten Personendaten» geht.

CH-Unternehmen bekennen sich (verbal) zum Datenschutz, praktisch setzt man ihn aber nicht wirklich um...

Neue Erkenntnisse - 180 Tage nach Einführung

Das Gute an DSGVO

- Datenschutz ist eine «Compliance Angelegenheit» und sollte bis 2020 in jedem Unternehmen eingeführt sein. Wer einen guten Datenschutz will, benötigt eine gute, angemessene und wirtschaftliche Cyber-Security (Informationssicherheit) Art. 32 DSGVO
- Jetzt ist die Zeit gekommen für einen «Datenschutzverantwortlichen - DPO» in Ihrem Unternehmen. Sie haben ja auch einen Chief Digital Officer (CDO), oder?

Neue Erkenntnisse - 180 Tage nach Einführung

Beobachtete Verstösse (Abmahnungen) gegen die DSGVO

- Webseite mit Kontaktformular ohne SSL Verschlüsselung
- Ganz fehlende Datenschutzerklärung auf der Webseite
- Nutzung von Google Analytics ohne IP-Anonymisierung und sauberes Opt-In

Neue Erkenntnisse - 180 Tage nach Einführung

DSGVO Verstösse in Österreich bis 13.9.18

- 721 Beschwerden aller Art (Standard Datenschutz-Geschäft). **248** davon zu einen grenzüberschreitenden Datenverkehr. Pünktlich um Mitternacht kam die erste Beschwerde von Max Schrems, die wir dann an die zuständige Behörde in Irland weitergeleitet haben.
- **252 Meldungen eines «data breach».** Aber erst in **zwei** Fällen habe man die Unternehmen tatsächlich auftragen müssen, die Betroffenen darüber zu informieren.
- 58 amtswegige Prüfverfahren
- 1 Konsultationsverfahren nach Art. 36 DSGVO zu Dashcams in Autos
- 4 Anträge auf Genehmigung von Verhaltensregeln Art. 40 DSGVO
- 115 Verwaltungsstrafverfahren

Quelle: Dr. Schmidl (Stv. Leiter der Österreichischen Datenschutzbehörde)

Neue Aspekte für den SiBe oder DSB im Unternehmen

Herausforderungen für den DPO

- Erfüllen der DSGVO-Anforderungen
  - Erstellen einer Übersicht der Verarbeitungstätigkeiten mit Verantwortlichen (Art. 30 DSGVO)
  - Die neuen Rechte der betroffenen Personen erfüllen können (Auskunft, Löschung, etc.) (Art. 15 DSGVO)
  - Die Datenschutz-Folgenabschätzung in den Risiko-Prozess integrieren (Art. 35 DSGVO)
  - Innert 72 Std. einen Datenschutz-Vorfall melden können (PR, Juristen, technische Umsetzung) (Art. 33 DSGVO)
  - Outsourcing-Verträge überprüfen (Art. 28 DSGVO)
- Datenschutz GAP-Analyse erstellen
  - Aufzeigen der GAPs in Bezug auf die Umsetzung des Datenschutzes und Massnahmen definieren
  - Die Einwilligung der betroffenen Person ist äussert wichtig, wenn es keine gesetzliche Grundlage gibt. Dazu muss die Person transparent und verständlich über den Zweck der Datenverarbeitung informiert werden. Gründe für das Bearbeiten der Personendaten können auch vertraglicher Natur oder das Erfüllen einer Rechtspflicht (z.B. Geldwäschereigesetz, etc.) sein. Hier gilt es eine Abwägung zu treffen.

DPO
Data Protection Officer

Neue Aspekte für den SiBe oder DSB im Unternehmen

7 Gründe für professionellen Datenschutz

- Gesetzliche Vorgaben einhalten
- Kundenanforderungen erfüllen
- Grundrechte und Image bewahren
- Haftungsreduktion und Imageschutz
- Risiko- und Qualitätsmanagement
- Prozessoptimierung
- Organisations- und Mitarbeiterschutz

DPO
Data Protection Officer

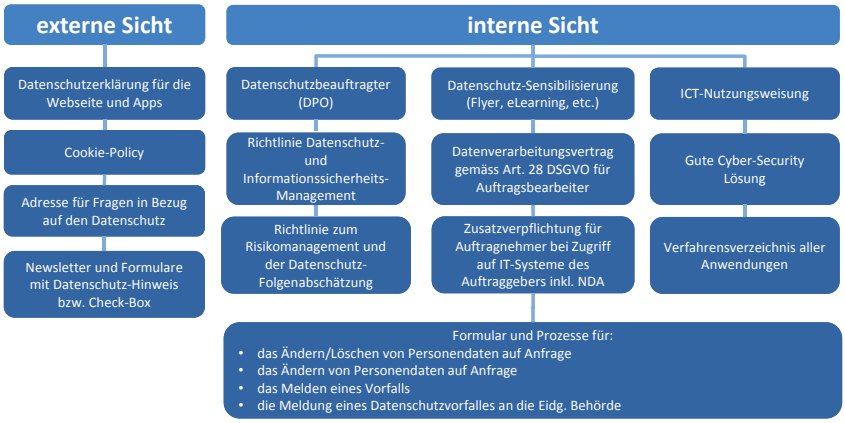
Neue Aspekte für den SiBe oder DSB im Unternehmen

Umsetzung

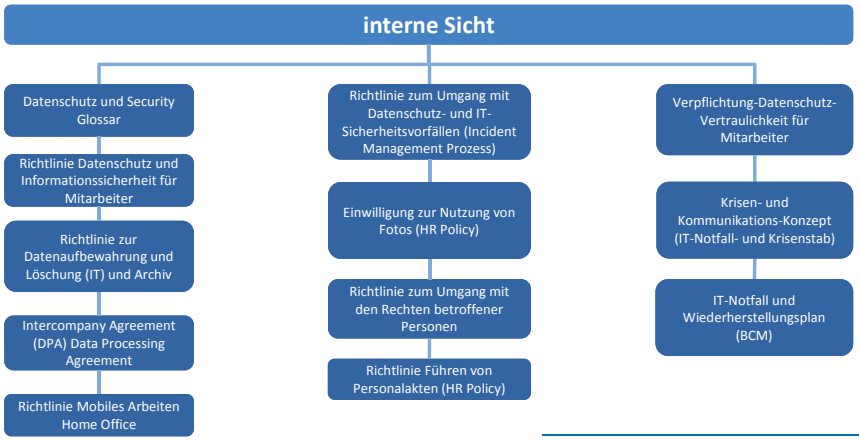
- Organisation
- Richtlinien und Weisungen
- Sensibilisierung aller Mitarbeitenden
- Nachweis- bzw. Dokumentationspflicht
- Prozesse und Formulare für die Ausübung der Rechte der betroffenen Personen

DPO
Data Protection Officer

Praktische Umsetzung 1/2



Praktische Umsetzung 2/2



Tipps und Tricks – Minimum Anforderungen

Was benötigen Sie um einen DSGVO/DSG-Datenschutz Audit zu bestehen?

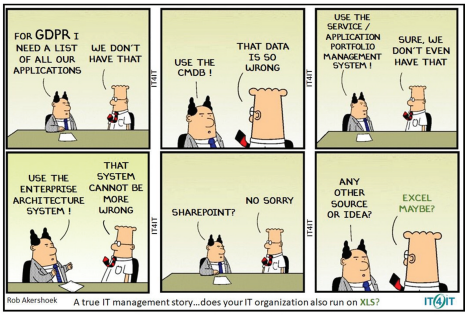
- Nachweis: Wie Sie sich als Unternehmen auf die DSGVO vorbereitet haben.
- Verzeichnis von Verarbeitungstätigkeiten
- Wie stellen Sie die Einhaltung der Betroffenenrechte (auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit) sicher.
- Wie stellen Sie sicher, dass Ihre technischen und organisatorischen Massnahmen bzw. die Ihrer Dienstleister ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten?
- Wie setzen Sie die Datenschutz-Folgenabschätzung um?
- Auftragsverarbeitung: Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern an die neuen Regelungen der DSGVO angepasst?
- Datenschutzbeauftragter: Wie ist dieser in Ihre Organisation eingebunden?
- Können Sie die Meldepflichten einhalten?
- Dokumentation: Können Sie die notwendigen Dokumente nachweisen?

Wer haftet für Datenschutzverstösse beim Einsatz von Video-Security, Zutrittskontrolle, Einbruchmeldetechnik?

- Wenn die Lösung von Ihnen betrieben wird, oder Sie die Lösung von einem Dienstleister betreiben lassen, sind Sie für den korrekten Betrieb zuständig und verantwortlich.
- Wenn Sie den Betrieb der Lösung extern in Auftrag gegeben haben, ist eine Zusatzvereinbarung nach Art. 28 DSGVO zu prüfen. In dieser wird geregelt, wie der Auftragsverarbeiter den Datenschutz mit technischen und organisatorischen Massnahmen sicherstellen kann. Ist dann wichtig, wenn der Auftragsverarbeiter unter die DSGVO fällt.
- Art. 82 DSGVO sieht die folgenden Haftungsregeln: „Jede Person, der wegen eines Verstosses gegen diese Verordnung ein materieller oder moralischer Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter.“ Deshalb haftet auch der Errichter/Installateur direkt gegenüber dem Geschädigten.
- Deshalb empfehle ich Ihnen, für jede Lösung ein **«Betriebskonzept» und Verträge mit dem Betreiber** zu erstellen und die Installation bzw. Wartung immer schriftlich zu dokumentieren. Vor der Installation solcher Security-Lösungen immer vorher die Anforderungen an den Datenschutz und die IT-Sicherheit klären.

Zusammenfassung

- 80/20 Regel anwenden
- Praktische Umsetzung
- Unterstützung bei Unsicherheit anfordern
- Ein Tool löst Ihre Probleme nicht
- Ruhe bewahren
- DSGVO = CH-DSG 2020



«Lieber 5 umgesetzte Massnahmen als 20 geplante»

«Herzlichen Dank für Ihre Aufmerksamkeit»

Wolfgang Sidler
SIDLER Information Security GmbH
Holzhäusernstrasse 5a | 6331 Hünenberg
wolfgang.sidler@sidler-security.ch
Tel: 041 781 57 72

SES
Verband Schweizerischer Errichter von Sicherheitsanlagen
Association Suisse des Constructeurs de Systèmes de Sécurité
Associazione Svizzera dei Costruttori di Sistemi di Sicurezza