DSGVO

Welche Auswirkungen für Walliser KMU ?

Stephan Kronbichler
M.B.L.-HSG
Rechtsanwalt
Savièse

KRONBICHLER & TOURETTE
AVOCATS • RECHTSANWÄLTE • ATTORNEYS-AT-LAW

Datenschutz-Grundverordnung

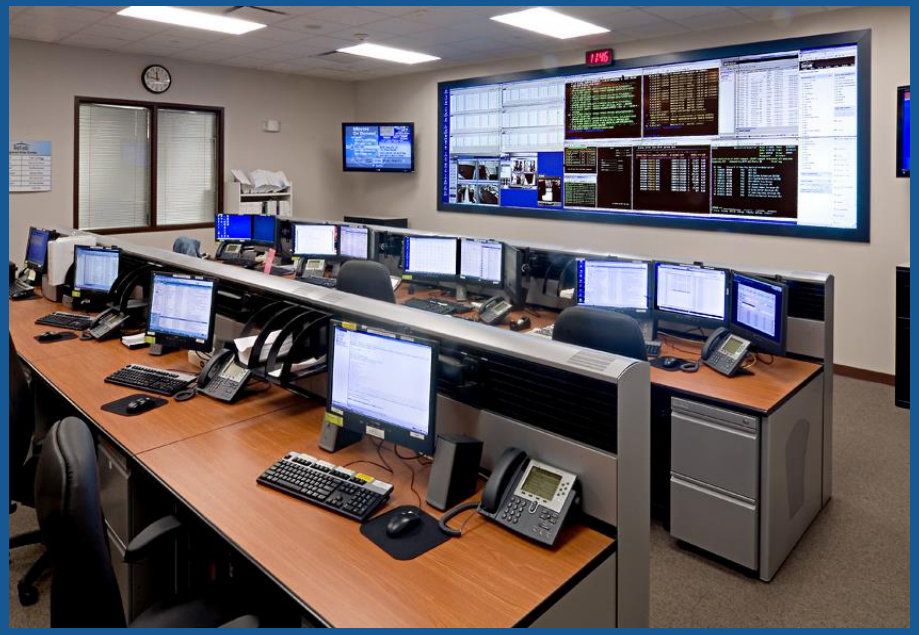
Richtlinie
95/46/EG

DSGVO

25.05.2018

Datenschutz-Grundverordnung

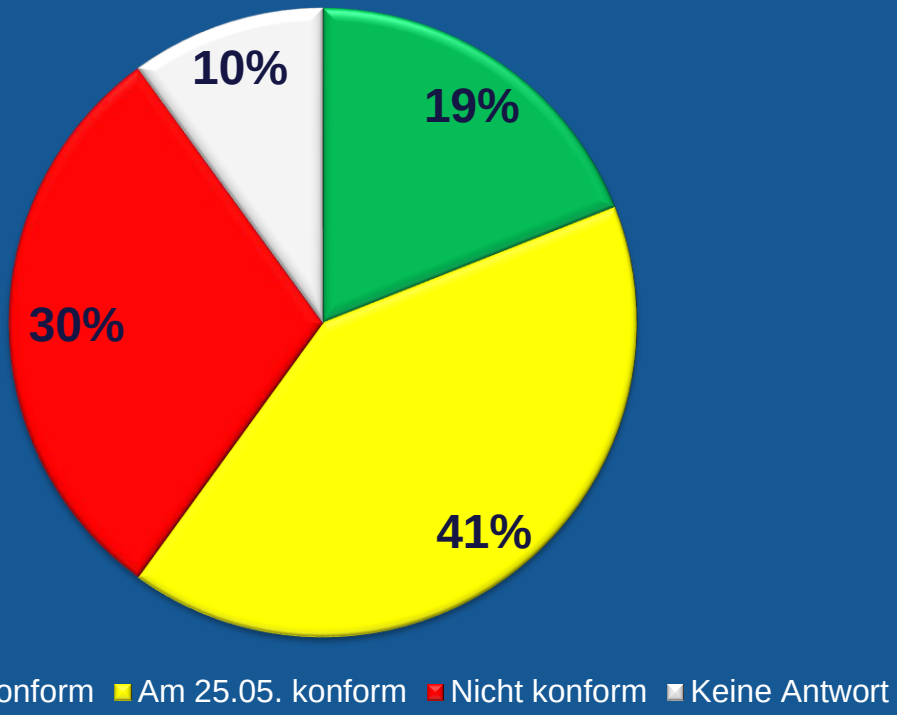
Datenbearbeitung vor DSGVO



Datenbearbeitung nach DSGVO

Datenschutz-Grundverordnung

Sind die Unternehmen bereit?



Quelle: Pierre Audoin Consultants (PAC), Moving beyond the GDPR, April 2018

Datenschutz-Grundverordnung

- Mehr als 70 Öffnungsklauseln für nationale Gesetze (mehr oder weniger streng, mehr Details)

- Wie viele der 28 EU-Mitgliedstaaten sind bereit (Gesetz in Kraft)?

  Nur 4 (Deutschland, Belgien, Österreich, Slovakei)![1]

→ Es gibt noch viele offene Fragen
→ Die Aufsichtsbehörden sind noch nicht bereit
→ Das Risiko einer spontanen Kontrolle ist daher gering…

[1] Quelle: International Association of Privacy Professionals, www.iapp.org, 24.04.2018

Datenschutz-Grundverordnung

- Die Grundprinzpien bleiben die selben!
- Die formellen Anforderungen nehmen stark zu, besonders für die Einholung der Einwilligung
- Die Informationspflichten sind viel umfassender
- Die Rechte der betroffenen Personen wurden verstärkt
- Verstösse können zu massiven Sanktionen führen

  → EUR 20’000’000 oder 4% des weltweiten Umsatzes !

Warum betrifft uns das überhaupt?

Warum betrifft uns das überhaupt?

Räumlicher Anwendungsbereich (Art. 3)

- Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung in der EU, egal ob die Verarbeitung in der EU oder ausserhalb stattfindet

- Verarbeitung von Daten von Personen, die sich in der EU befinden, durch einen nicht in der EU niedergelassenen Verantwortlichen, wenn die Datenverarbeitung im Zusammenhang steht mit dem
  a) Anbieten von Waren oder Dienstleistungen, auch gratis
  b) Beobachten des Verhaltens der Personen, soweit das Verhalten in der Union erfolgt

Warum betrifft uns das überhaupt?

Räumlicher Anwendungsbereich (Art. 3) (Forts.)

Anbieten von Waren oder Dienstleistungen: Indizien

- ✓ Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen
- ✓ Erwähnung von Kunden oder Nutzern, die sich in der EU befinden

- Nicht blosse Zugänglichkeit der Website in der EU
- Nicht schon die Verwendung einer Sprache, die im Land des Verantwortlichen allgemein gebräuchlich ist

Warum betrifft uns das überhaupt?

Räumlicher Anwendungsbereich (Art. 3) (Forts.)

Beobachtung des Verhaltens:

- ✓ Nachvollzug der Internetaktivität einer natürlichen Person
- ✓ Verwendung von Techniken zur Erstellung eines Profils der Person als Grundlage für sie betreffende Entscheidungen bzw. zur Analyse oder Vorhersage ihrer persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten

→ Cookies, Google Analytics, dynamic pricing, etc.

Einige Worte zum Inhalt

Personenbezogene Daten (Art. 4)

- Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

- Identifizierbar: direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind

→ IP-Adressen sind Personendaten (vgl. BGE 136 II 508)

→ DSGVO betrifft nicht die Daten von juristischen Personen

Grundsätze (Art. 5)

- Rechtmässigkeit (Einwilligung, Vertrag, überwiegendes Interesse)
  → Einwilligung: freiwillig, konkret, informiert, durch aktive Handlung
- Verarbeitung nach Treu und Glauben
- Transparenz
- Festgelegter, eindeutiger und legitimer Zweck
- Verhältnismässigkeit (Datenminimierung)
- Richtigkeit
- Sicherheit

→ DSG / DSGVO: 77 Artikel auf ca. 40 Seiten
→ DSGVO: 99 Artikel auf 88 Seiten… plus nationale Gesetze !

Informationspflicht (Art. 13 und 14)

Mitzuteilende Informationen :

- Namen und Kontaktdaten des Verantwortlichen sowie seines Vertreters
- Kontaktdaten des Datenschutzbeauftragten
- Kategorien personenbezogener Daten, die verarbeitet werden
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen
- Rechtsgrundlage für die Verarbeitung
- Aus welcher Quelle die personenbezogenen Daten stammen
- Empfänger oder Kategorien von Empfängern
- Ob eine Übermittlung ins Ausland erfolgt, und zu welchen Bedingungen
- Aufbewahrungsdauer oder mindestens die Kriterien für die Festlegung dieser Dauer
- Erwähnung der diversen Rechte der betroffenen Person (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht, Datenübertragbarkeit)
- Erwähnung des Beschwerderechts bei einer Aufsichtsbehörde
- Erklärung, ob die Einwilligung für einen Vertragsabschluss erforderlich ist
- Bestehen einer automatisierten Entscheidungsfindung

Informationspflicht (Art. 13 und 14)

Zentraler Punkt, der eine Reaktion erfordert!

- → Einwilligungserklärungen prüfen und ggf. ergänzen, auch z.B. in den Kundenverträgen
- → Prozess zur Einholung der Einwilligung prüfen und ggf. anpassen
- → Information bei Beschaffung der Daten sicherstellen
- → Allgemeine Information auf der Website publizieren

Was soll ich jetzt konkret tun?

Was soll ich jetzt konkret tun?

- Die Grundsätze ändern kaum, die formellen Aspekte dagegen stark
  - → Verzeichnis der Verarbeitungstätigkeiten
  - → Informationspflicht, Einwilligung
  - → Verträge mit Auftragsverarbeitern

→ Die DSGVO enthält viele einfach zu kontrollierende Checklisten

- Risikobasierter Ansatz der DSGVO und des DSG
  - → Ziel ist nicht «Note 6» zu einem astronomischen Preis
  - → Treffen von angemessenen Massnahmen, gestützt auf bewusste und dokumentierte Entscheide

Was soll ich jetzt konkret tun?

- ❑ Inventar aller Datenverarbeitungen im Unternehmen erstellen
  - → Kunden, Lieferanten, Mitarbeiter, etc.
  - → Doppelte Kontrolle: Prozesse und Systeme
- ❑ Dokumentieren
  - → Welche Daten, über wen, woher, durch wen, auf welcher Grundlage (Rechtfertigung), zu welchem Zweck, auf welchen Systemen, wie lange, an wen übermittelt (ins Ausland)?
  - → Technische und organisatorische Schutzmassnahmen (TOM)
- ❑ Strukturieren und Prioritäten definieren
  - → Alle nicht benötigten Datenbearbeitungen eliminieren (Doubletten, überholte Daten, etc.)
  - → Für die Übrigen die nötigen Massnahmen zur Herstellung der Konformität ermitteln
  - → Heikelste und deshalb prioritär zu regelnde Datenbearbeitungen identizifieren (Bedeutung für das Unternehmen, Menge/Art der Daten, grösste Unordnung, mit den grössten Risiken verbunden, …)

Was soll ich jetzt konkret tun? (Forts.)

- Vertragsdokumente anpassen
  - → Einwilligungserklärungen (→ mit den nötigen Informationen ergänzen), inkl. Prozess zur Einholung (→ kein bereits angekreuztes Kästchen!)
  - → Privacy Policy → vervollständigen → veröffentlichen
  - → Verträge mit Lieferanten (Outsourcing)
  - → Datentransferverträge mit Dritten oder im Konzern

Was soll ich jetzt konkret tun? (Forts.)

Verträge mit Auftragsverarbeitern

Kunde (Verantwortlicher)	**Auftragsverarbeiter**
Garantiert die Rechtmässigkeit (Erhebung / Einwilligung, Zweck, Bearbeitung gem. Vertrag, Weisungen)	Bearbeitet die Daten nur gemäss Vertrag
Bestätigt, dass die technischen und organisatorischen Massnahmen (TOM) angemessen sind → TOM als Anhang zum Vertrag aufnehmen	Implementiert TOM und wendet diese an
Stellt Einhaltung der Rechte betroffener Personen sicher (Auskunft, Löschung, etc.)	Leitet Anfragen weiter, unterstützt den Kunden, ggf. gegen separate Vergütung
Muss Einhaltung des Datenschutzes nachweisen	Liefert alle dafür nötigen Informationen und erlaubt Prüfungen vor Ort
Ist Ansprechpartner der Aufsichtsbehörden	Leitet Anfragen an den Kunden weiter

Was soll ich jetzt konkret tun? (Forts.)

- Vertragsdokumente anpassen
  - → Einwilligungserklärungen (→ mit den nötigen Informationen ergänzen), inkl. Prozess zur Einholung (→ kein bereits angekreuztes Kästchen!)
  - → Privacy Policy → Vervollständigen → Veröffentlichen
  - → Verträge mit Lieferanten (Outsourcing)
  - → Datentransferverträge mit Dritten oder im Konzern
- Prozesse aufsetzen bzw. vervollständigen
  - → Prozesse zur Einhaltung der Rechte der betroffenen Personen (Anfragen um Auskunft, Portabilität, Berichtigung, Löschung, Einschränkung, Widerspruch)
  - → Prozess zur Reaktion auf Datenschutzverletzungen (insbesondere Information, Korrekturmassnahmen)
- Technische und organisatorische Schutzmassnahmen anpassen, falls nötig
- Ev. Vertreter in der EU benennen (Art. 27)
  - → Ad hoc-Tochtergesellschaft, die zur Not geopfert werden könnte

Zum Schluss…

Zum Schluss…

- → Keine Panik, es ist sowieso zu spät
- → Sie sind bei weitem nicht der Einzige, und es gibt viel lohnendere Ziele
- → Mit wenig Aufwand lässt sich schon viel erreichen
  - Die DSGVO enthält viele ‘Checklisten’, z.B. abzugebende Informationen, Inhalt von Auftragsverarbeitungsverträgen, etc.
  - Den Text der Einwilligungserklärung und die Privacy Policy kann man sehr einfach anpassen
  - Viele TOMs kann man durch Auslagerung an einen professionellen, zertifizierten Provider leicht implementieren

Fragen und Antworten

Stephan Kronbichler
Rechtsanwalt
Kronbichler & Tourette
Boulevard des Philosophes 17
Postfach 507
1211 Genf 4

Nach Vereinbarung:
Rue des Remparts 13
1950 Sitten

Tel. +41 22 705 11 22
Fax +41 22 705 11 21
Mobile +41 78 665 81 34

stephan.kronbichler@kt-legal.ch
www.kt-legal.ch

KRONBICHLER & TOURETTE

AVOCATS • RECHTSANWÄLTE • ATTORNEYS-AT-LAW