Homburger

EU Datenschutz-Grundverordnung

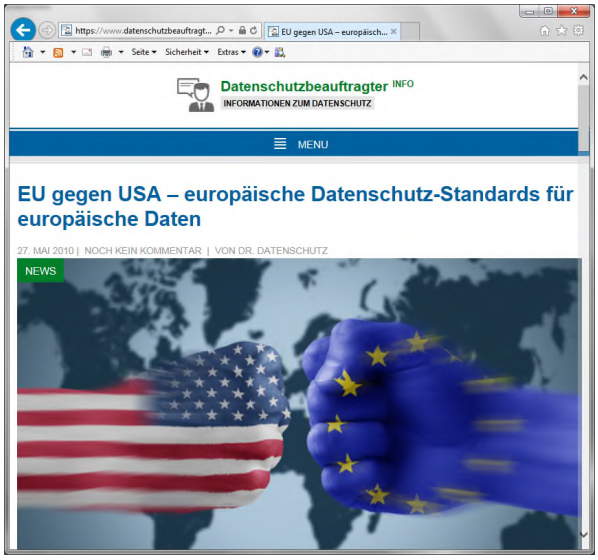
Workshop für Unternehmen in der Schweiz

David Rosenthal

13. Juni 2016

Version 2.01

Homburger



Eine Lex Facebook & Co., die generalisiert wurde …

Homburger

facebook

Artikel 20

Recht auf Datenübertragbarkeit

(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

PS. Ist Facebook mit Bezug auf diese Daten überhaupt ein "Verantwortlicher"?

… voller unklarer Regelungen

Homburger

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags,

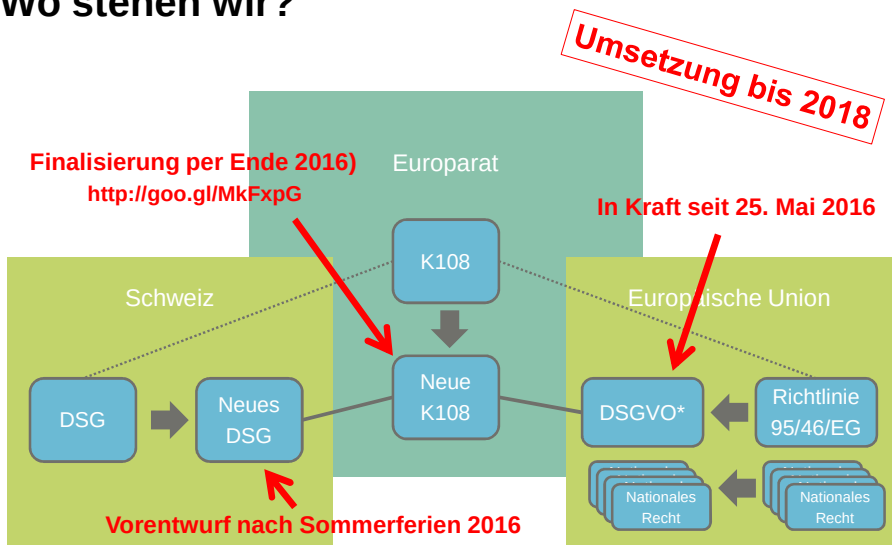
Art. 7 Abs. 4 DSGVO

(8) Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, müssen sie maschinenlesbar sein.

Art. 12 Abs. 8 DSGVO

Homburger

Wo stehen wir?



* Datenschutz-Grundverordnung

Homburger

Wesentliche Punkte

- **Grundkonzept** (was ist erlaubt, was nicht) bleibt dasselbe
  - EU verlangt für jede Datenbearbeitung eine Rechtfertigung (z.B. Einwilligung, Erfüllung einer Rechtspflicht, berechtigte Interessen) (im DSG ist das anders)
- **Räumlicher Geltungsbereich:** Die DSGVO gilt auch für viele Schweizer Firmen
- **Personendaten:** Werden unter der DSGVO anders verstanden als im DSG
- **Einwilligung:** Die Anforderungen an ihre Gültigkeit sind gestiegen
- **Informationspflichten:** Es muss wesentlich umfassender informiert werden
- **Betroffenenrechte:** Betroffene erhalten neue Eingriffs- und Auskunftsrechte
- **Governance:** Der Aufwand insbesondere bezgl. der Dokumentation steigt
- **Buzzwords:** Privacy by Design & Co. – meist alter Wein in neuen Schläuchen
- **Auslandsdatentransfer:** Hier bleibt im Wesentlichen alles beim Alten
- **Sanktionen:** Scharfe Sanktionen – aber in der Schweiz kaum durchzusetzen?
- **Frist zur Umsetzung:** 25. Mai 2018

Homburger

Gap Analyse: Vieles vergleichbar

EU General Data Protection Regulation vs. Swiss Data Protection Act (in the Private Sector[1])

June 13, 2016 | Version 3.01 | David Rosenthal (david.rosenthal@homburger.ch) | Updates and more infos: http://www.homburger.ch/dataprotection

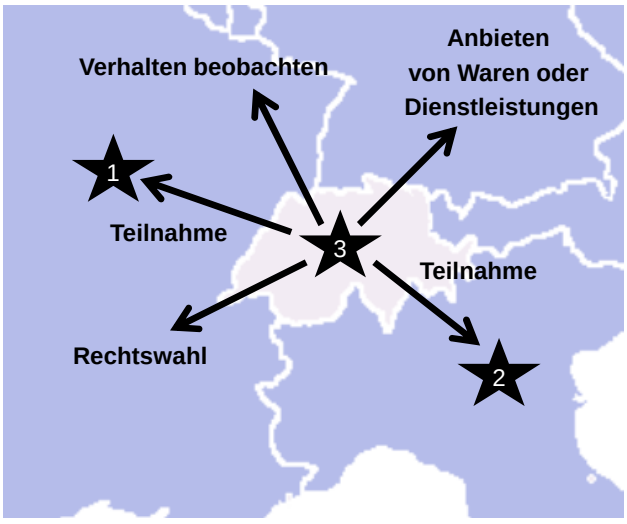
EU GDPR	Art.	CH DPA is ...	Art. DPA	Main differences	Change in CH DPA likely?[2]
Material scope	2	Comparable	2	GDPR excludes all purely personal and household activities from scope	
Territorial scope	3	Comparable	PILA 139	DPA has slightly broader territorial applicability	
Definitions	4	Comparable	3	DPA defines personal data slightly narrower as to when a person is identifiable (follows a "relative approach"), but includes data of legal persons as well GDPR states that consent must be "freely given, specific, informed and unambiguous" to be valid, which corresponds to the current definition of consent under the DPA; however, the GDPR defines consent by affirmative action more narrowly than under the DPA (*e.g.*, no pre-ticked boxes)	
Principles of processing**	5	Comparable	4, 5, 7	GDPR is express on specific aspects of proportionality (such as data minimization and data retention)	Yes

[1] Excluding provisions on processing by public authorities and excluding provisions concerning authorities and procedures in the Union (*e.g.*, coordination among supervisory authorities)
[2] The planned changes in the context of the ongoing revision of the DPA are not yet known. A pre-draft for public comment is expected following the summer break 2016. Based on the requirements of the revised Council of Europe Convention 108, this column indicates in which areas we expect a change to the DPA (depending on how narrow these requirements are interpreted by the Federal Administration).

Gap Analyse zum DSG abrufbar unter http://www.homburger.ch/dataprotection

Homburger

Wer fällt unter die DSGVO?



1 Controller*

2 Processor**

3 Controller oder Processor

* "Verantwortlicher"

** "Auftragsverarbeiter"

Homburger

Wer fällt unter die DSGVO?

- **Viele Schweizer Unternehmen werden erfasst sein**
  - Wer an Datenbearbeitungen von EU-Unternehmen teilnimmt (Konzern)
  - Wer auch Daten von Kunden bearbeitet, die sich in der EU befinden
  - Wer die Aktivitäten von Besuchern seiner Website | seines Apps analysiert
- **Aber: Es gelten nicht dieselben Regeln wie für EU-Unternehmen**
  - Konzept der "federführenden Aufsichtsbehörde" (One-Stop-Shop) gilt nicht, d.h. jede Aufsichtsbehörde kann konkurrierend agieren (Territorialitätsprinzip)
  - Möglicherweise keine Berufung auf im sonstigen EU-Recht verankerte Ausnahmeregelungen und Rechtfertigungen (z.B. Art. 6(1)(c), 22(2) und 23)
  - Direkte Durchsetzung von Administrativmassnahmen gegen Unternehmen in der Schweiz ist fraglich (ihre Rechtsnatur wird aber je nach Land variieren)
  - Pflicht ausländischer Unternehmen zur Benennung einer Person in der EU, die sie "in Bezug auf ihre Pflichten" unter der DSGVO "vertritt" (vgl. Erw. 80)

Homburger

À propos Sanktionen …

- Jede (nationale) Aufsichtsbehörde kann **Administrativsanktionen** erlassen
  - Sie sollen im Einzelfall "wirksam, verhältnismässig und abschreckend" sein
  - Bei Governance|Kinderdatenschutz: EUR 10 Mio. oder 2% des weltweiten Umsatz (des Unternehmens, nicht der Gruppe; es gilt der höhere Wert)
  - Beim materiellen Datenschutz: EUR 20 Mio. oder 4% des weltweiten Umsatz
- Wo Administrativsanktionen nicht möglich sind, sind **andere Sanktionen** erlaubt
- Aufsichtsbehörden haben **Verfügungsgewalt gegen Datenbearbeitungen**
  - Bearbeitungen können vorübergehend oder dauernd unterbunden werden
  - Sie sind zugleich verpflichtet, Beschwerden von Betroffenen zu bearbeiten
- Betroffene können **Ansprüche** (z.B. Schadenersatz) **gerichtlich** durchsetzen
  - Vereine können im Namen von Betroffenen wie auch eigenständig klagen
- **Achtung:** Auch im DSG werden Administrativsanktionen erwartet (10% wie KG)

Homburger

Den Esel meinen, den Sack schlagen?

— Welche **persönliche Verantwortlichkeit** kommt dem "Vertreter" zu?

(17) „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

— **Variante 1:** Rechtsvertreter und Zustelldomizil (Beispiel: Anwalt)
— **Variante 2:** Stellvertretender Verantwortlicher (Beispiel: Prüfperson gem. KlinV)
— Frage bisher ungeklärt; Argument der Durchsetzbarkeit spricht für Variante 2
— Im Falle von Variante 2 bietet sich Gründung eines **Special Purpose Vehicle** in der EU an, das im Bedarfsfall geopfert werden kann (oder Art. 27 wird ignoriert)

Homburger

Wer braucht *keinen* Vertreter in der EU?

(2) Die Pflicht gemäß Absatz 1 des vorliegenden Artikels gilt nicht für

(a) eine Verarbeitung, die gelegentlich erfolgt, nicht die umfangreiche Verarbeitung besonderer Datenkategorien im Sinne des Artikels 9 Absatz 1 oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, oder

(b) Behörden oder öffentliche Stellen.

Besonders schützenswerte Personendaten

Kriterien müssen kumulativ erfüllt sein, jedoch nur in Bezug auf die Bearbeitung von Daten von Personen, die sich in der EU befinden

Homburger

Personendaten

(1) „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die 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, [illegible] schen, genetischen, psychischen, [illegible] chen, kulturellen oder sozialen Identitä türlichen Person sind, identifiziert werd

Die EU verfolgt zusehends den "absoluten" Ansatz beim Begriff der Personendaten, wenngleich unsystematisch und in einer widersprüchlichen Weise …

(30) Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.

Im Schweizer DSG gilt bei praktischer gleicher Definition der "relative" Ansatz, bestätigt in BGE 136 II 508 (Logistep)

Homburger

Einwilligung

— **Relevanz:** Neben der Vertragserfüllung, gesetzlichen Pflicht und "berechtigten Interessen" die wichtigste Grundlage zur Bearbeitung von Personendaten

(11) „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Eine in einem Vertrag vorgesehene Einwilligung für eine Datenbearbeitung sollte optional sein, wenn sie für die Vertragserfüllung nicht nötig ist (Art. 7(4))

— Definition entspricht dem **Schweizer Verständnis** einer gültigen Einwilligung
— Einwilligungstext muss von anderen Themen **getrennt dargestellt** werden
— **Rückzug** jederzeit möglich (mit Wirkung *pro futuro*, aber ggf. Löschanspruch)
— Bisher gültige Einwilligungen müssen nicht neu eingeholt werden

Homburger

Informationspflichten

- **Grundsatz der Transparenz** wird ergänzt durch **eine Informationspflicht mit definiertem Mindestinhalt**
  - Soweit Betroffene nicht schon anderweitig informiert worden sind
  - Gilt auch bei indirekter Datenbeschaffung (Frist: max. 1 Monat), ausser wo die Information unmöglich oder unverhältnismässig wäre oder den verfolgten Zweck vereiteln würde (dann sind Alternativen wie z.B. Web-Infos zu prüfen)
  - Informationspflicht auch bei späterer Zweckänderung
- **Folge:** Umfassende Datenschutzerklärungen für die Betroffenen werden Pflicht
  - Bei Erstkontakt bzw. Datenbeschaffung
  - Auf der eigenen Website für alle nicht erfassten Fälle indirekter Beschaffung
  - Wenige Ausnahmen wie z.B. interne Untersuchungen
- **Pro memoria:** Informationspflicht auch bei gewissen Datenschutzverstössen

Homburger

Worüber informieren?

- Name, Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten
- Bearbeitungszwecke, Datenkategorien, etwaige Datenempfänger (Kategorien)
- Berechtigte Interessen, sofern darauf abgestellt wird
- Ob Export beabsichtigt ist, ob in ein sicheres Drittland und falls nicht, wo etwaige Garantien zur Sicherstellung des Datenschutzes eingesehen werden können
- Quelle der Daten (falls nicht beim Betroffenen direkt erhoben)
- Dauer der Datenspeicherung (oder wie sie bestimmt wird)
- Hinweis auf Recht der Betroffenen auf Auskunft, Berichtigung, Löschung, Beschränkung, Widerspruch und Datenportabilität
- Möglichkeit zum Widerruf einer etwaigen Einwilligung (und ggf. die Folgen)
- Beschwerderecht bei einer Aufsichtsbehörde
- Ob die verlangten Daten für eine Vertragserfüllung erforderlich sind und was geschieht, wenn die Betroffenen die Daten nicht offenlegen
- Automatisierte Einzelfallentscheide (inklusive Profiling), deren Logik und Folgen

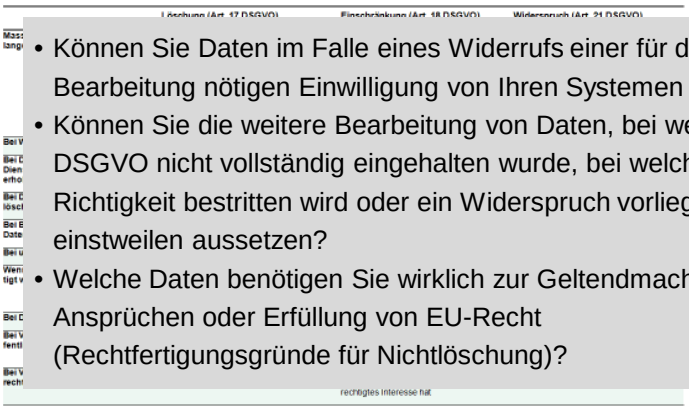
Homburger

Betroffenenrechte

- Die Rechte der Betroffenen werden deutlich **ausgebaut** und verkompliziert
  - Unklar ist, wie sehr sie in der Praxis tatsächlich beansprucht werden
  - Erfordern **Anpassungen** an Abläufen und Systemen eines Datenbearbeiters
- Anträge müssen **unentgeltlich** und **innert Monatsfrist** erfüllt werden
  - Fristverlängerung um zwei Monate möglich
  - Bei "offenkundig unbegründeten" oder "exzessiven" Anträgen kann ein angemessenes Entgelt verlangt oder die Erfüllung verweigert werden
  - Frühere Empfänger der Daten müssen ggf. ebenfalls informiert werden
- Anspruch auf **Auskunft** und **Datenportabilität** (= Rückgabe eigener Daten)
- Recht auf **Berichtigung**
- Recht auf **Löschung** ("Recht auf Vergessen"), **Einschränkung** (= teilweises Benutzungsverbot) und **Widerspruch** (= vollständiges Benutzungsverbot)
- Recht auf **"menschliches" Gehör** bei automatisierten Einzelfallentscheiden

Homburger

Löschung, Einschränkung und Widerspruch



- Können Sie Daten im Falle eines Widerrufs einer für die Bearbeitung nötigen Einwilligung von Ihren Systemen löschen?
- Können Sie die weitere Bearbeitung von Daten, bei welchen die DSGVO nicht vollständig eingehalten wurde, bei welchen deren Richtigkeit bestritten wird oder ein Widerspruch vorliegt, einstweilen aussetzen?
- Welche Daten benötigen Sie wirklich zur Geltendmachung von Ansprüchen oder Erfüllung von EU-Recht (Rechtfertigungsgründe für Nichtlöschung)?

Übersicht abrufbar unter http://www.homburger.ch/dataprotection

Homburger

Datenportabilität

- **Welche Voraussetzungen müssen vorliegen (kumulativ)?**
  - Eigene Personendaten
  - Einem Verantwortlichen übergeben (nicht bloss Auftragsverarbeiter!)
  - Bearbeitung erfolgte gestützt auf eine Einwilligung oder einen Vertrag
  - Bearbeitung erfolgte mithilfe automatisierter Verfahren
  - Rechte anderer Personen werden durch die Rückgabe nicht beeinträchtigt
- **Was kann der Betroffene verlangen?**
  - Rückgabe der Daten in "strukturierter, gängiger, maschinenlesbarer" Form
  - Soweit technisch machbar die direkte Übermittlung der Daten an einen anderen Verantwortlichen (Nachfolger), der die Daten weiterbearbeiten soll
- **Atypische Anwendungsfälle noch unklar** (im Auge waren Facebook & Co.)
  - Ärzte (Patientendaten)? Banken (Aufträge)? Online-Shops (Bestellungen) ? Auktionsplattformen (Angebote)? Arbeitgeber (Online-Bewerbungen)?

Homburger

Einzelfallentscheide, Profiling

- **Verbot** oder blosses **Widerspruchsrecht**?

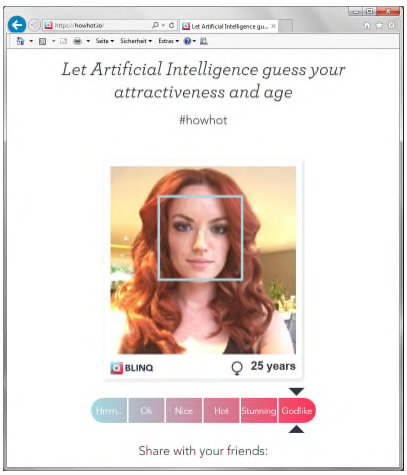
(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Die Bestimmung zielt auf vollautomatische Kredit- oder Anstellungsentscheide, findet aber viel breitere Anwendung, z.B. auf personalisierte Preise, Online-Software-Aktivierung oder Sicherheitsüberwachung

- **Option 1:** Profiling bzw. Einzelfallentscheide werden nur benutzt, wo sie keine rechtlichen oder erheblichen Folgen haben (z.B. personalisierte Werbung)
- **Option 2:** Profiling bzw. Einzelfallentscheide werden nur für den Abschluss oder die Abwicklung eines Vertrags benutzt, ohne sensitive Daten, und die betroffene Person hat mind. das Recht, über Entscheide mit einem Menschen zu sprechen
- **Option 3:** Es werden eine explizite Einwilligung eingeholt und Vorkehrungen im Fall eines Widerrufs getroffen; das "menschliche" Gehör braucht es trotzdem

Inskünftig datenschutzwidrig?

Homburger



Quellen: http://faces.ethz.ch, Google, http://www.dailymotion.com/video/xg078_robot-sentinella

Governance

Homburger

— Prinzip der "**Accountability**": Verantwortlicher trägt "Beweislast" für Compliance

— Verträge mit **Auftragsverarbeitern**: Neu detaillierte Vorgaben an Vertragsinhalt, aber keine wesentlichen Änderungen (Ausnahme: Vetorecht bei Subprocessors)

— **Verzeichnis der Verarbeitungstätigkeiten** ist neu zwingend zu führen, auch von Auftragsvearbeitern; Inhalt entspricht etwa dem, was nach Art. 11a DSG zu registrieren oder intern zu führen ist, plus Angaben über Exporte, die Dauer der Datenaufbewahrung und zu technischen und organisatorischen Massnahmen

— Vornahme einer formalen und definierten Vorgaben gemäss DSGV folgenden **Datenschutz-Folgenabschätzung** bei Vorhaben mit vermutlich hohen Risiken; ist das Risiko in der Tat hoch, ist die **Datenschutzbehörde** zu **konsultieren**

— Firmen, deren Geschäft auf der Überwachung von Personen oder sensitiven Personendaten basiert, müssen einen **Datenschutzbeauftragten** benennen

Homburger

Data Breach Notifications

- Alle Verstösse gegen Massnahmen zum Schutz von Daten müssen neu **verzeichnet** werden und – wenn Auswirkungen auf Betroffene möglich sind – der **Datenschutzbehörde** sofort (innert 72 Stunden) **gemeldet** werden
  - Was ist passiert? Wer ist betroffen? Folgen? Massnahmen? Kontakt?
  - Im Fokus stehen Verletzungen von IT-Sicherheit (Hacker, Datenverluste, falsch versendete E-Mails, vertauschte Rechnungen), aber erfasst sein können auch sonstige Regelverstösse (z.B. weisungswidrige Datennutzung)
- **Information an Betroffene** ist bei einem hohen Risiko von Auswirkungen nötig
  - Nicht nötig im Falle von Massnahmen um Zugriffe durch Dritte zu verhindern (verschlüsselte Daten) oder die das Risiko nach aller Wahrscheinlichkeit eliminiert haben
  - Falls die individuelle Information zu aufwändig ist: Publikation oder andere Massnahme um betroffene Personen "vergleichbar wirksam" zu informieren

Homburger

Des Datenschützers liebste Schlagworte …

- **Datenminimierung** (Art. 5)
  - Daten sollen dem Zweck angemessen, erheblich sowie auf das für den Zweck der Verarbeitung notwendige Mass beschränkt sein (f.k.a. "Grundsatz der Verhältnismässigkeit")
- **Privacy by Design** (Art. 25)
  - "… geeignete technische und organisatorische Massnahmen …, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen …"
- **Privacy by Default** (Art. 25)
  - "… trifft geeignete technische und organisatorische Massnahmen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden …"

Homburger

Privacy by Design

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Z... legung der M...

1 Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

...ganisatorische Maß... ...wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Alles klar?

Einfacher: Art. 7 Abs. 1 DSG

Homburger

Auslandsdatentransfers

- **Die gute Nachricht:** Heute zulässige Datentransfers ins Ausland sind vom Prinzip her auch unter der DSGVO zulässig
  - Konzept der **Angemessenheitsbeschlüsse** bleibt
    - Bisherige Beschlüsse behalten ihre Gültigkeit; Schweiz hat bei Einhaltung der Konvention 108 an sich Anspruch auf Annahme der Angemessenheit
  - Konzept **vertraglicher Garantien** und **Binding Corporate Rules** (BCRs) bei Exporten in unsichere Drittländer besteht weiterhin (trotz Safe-Harbor-Urteil)
    - BCRs müssen weiterhin behördlich genehmigt werden
    - EU-Standardklauseln gelten weiterhin (dürften aber noch revidiert werden)
- Neu können Exporte in unsichere Drittländer auch auf Basis von genehmigten "**Code of Conducts**" und genehmigten **Zertifizierungsmechanismen** erfolgen
- Für Exporte aus der Schweiz sind diese Bestimmungen nur teilweise relevant
  - Zudem erlaubt schon das heutige DSG die Nutzung der EU-Instrumente

Homburger

Und wie umsetzen?

Homburger

Situation "vor" DSGVO

1 Really must have

Intra-Group Data Transfer Agreement (IGDTA)

Multilateral data agreement that regulates Group internal cross-border and outsourcing transfers

Serves a nucleus for establishing a global data protection governance framework

Ability to cover all data within the company as well as all entities ("big bang" or "step-by-step")

A proven, cost effective approach already followed by many other multinationals

Recognized by the European Commission and the European data protection authorities

Roll-out possible within six months (if no local pushback)

Does not limit Group companies in the processing of their *own* data; it only sets forth rules on how they have to treat data of other Group companies and does so based on Group policies

Appointment of local data protection coordinator for local implementation and notifications with authorities

2 Must have

Group data protection policies

Establishing group-wide data protection policies step-by-step

Start with a general data protection policy, then continue with policies for key areas and applications such as HR, data from website and consumers

Local law adjustments where required

Definition of responsibilities for data protection compliance (1st, 2nd and 3rd line of defense), including local law obligations (e.g., local registrations|filings)

Group-wide data protection training program for dealing with personal data

Integration of policies into the IGDTA framework, local management to put in place policies

As opposed to the IGDTA, the policies define standards that Group companies must abide to also for their own personal data (e.g., HR data), even when stricter than local law

3 Should have

Inventory of data files and data processing procedures

Centrally documented the way how the Group and its entities is collecting, using, storing, disclosing and otherwise processing personal data

Centrally documented Group data protection compliance, including local authority filings, etc.

Part of this task will have to be done already for the purpose of creating data protection policies

Also focusing on decentralized data files since they are likely to be processed with less care and coordination than in the case of Group wide applications

Task requires local assistance; can be performed by the local data protection coordinator

Allows early identification of data protection issues

Easier compliance with legal standards (e.g., obligation to notify or register with data protection authorities)

4 Good to have

Data Protection Officer and standardization of compliance procedures

Key procedures|tasks to ensure compliance with data protection policies and legal requirements are standardized (instead of ad-hoc and potentially inconsistent handling of issues)

Shall cover data subject access requests, data protection review of new projects, IT applications and reviews of third party contracts for data protection compliance

Creation of standard clauses for service provider contracts, data subject requests, etc.

Group data protection officer as a center of competence with a network of local data protection compliance managers

Early identification of Group internal data protection issues and developments in the legal environment and ability to approach them strategically

Defined procedures for regular audits of Group entities and service providers

5 Nice to have

Data Protection Management System (DPMS)

Implement a Group wide data protection management system, i.e. the necessary documentation and processes to ensure that data protection compliance (prevent, detect, respond violations) is done systematically instead of ad-hoc and that any need for changes to the processing of data is addressed early on

All procedures involving the processing of personal data have been documented, have been reviewed and adapted for compliance with applicable data protection laws and group policies and the IGDTA, where stricter, and are periodically reviewed for improvement

All systems used for processing personal data shall provide an adequate level of data security in line with the recommended controls and measures as per the ISO 27001 standard

Eventually, the Group may have certain aspects of its data protection compliance externally audited and certified

Homburger

Ausgangslage

- Mehrheit der Unternehmen haben **maximal die Stufe 1 oder 2** erreicht
  - Keine durchgängige Datenschutz-Governance
  - Datenschutz wird *ad hoc* betrieben, wenn auch ohne grössere Probleme
- Die drei grössten **Herausforderungen**
  - Zusammentragen und Ordnen der für eine Beurteilung nötigen Informationen
  - Fehlende personelle Ressourcen und Kooperation (IT, Business, Legal)
  - Anpassung von IT-Systemen und Geschäftsprozessen und ggf. Verzicht auf bestimmte Datenbearbeitungen, die sich nicht mehr rechtfertigen lassen
- **Druck seitens Top-Management** aufgrund von Administrativsanktionen
- **Aber:** DSGVO verfolgt und verlangt einen **risikobasierten Ansatz** (gemeint ist das Risiko der Verletzung der Datenschutzrechte der betroffenen Personen)
  - Kein Unternehmen wird die DSGVO in jeder Hinsicht einhalten (können)

Homburger

Vorgehensweise 1|2

- **Strategie der DSGVO-Compliance festlegen**
  - Soll die DSGVO nur wo nötig umgesetzt werden oder soll sie den neuen "Standard" im Unternehmen definieren? Daten juristischer Personen?
  - Zentrale Projektführung oder Delegation an die Ländergesellschaften?
  - Gesellschaftsrechtliche Massnahmen zur Begrenzung des Risikos?
- **Prioritäten setzen**
  - Sich zuerst die wirklich heiklen Bearbeitungen vornehmen
    - Welches sind die heikelsten Datenbearbeitungen?
    - Wo droht dem Unternehmen am ehesten Ungemach?
  - Zuerst jene Anpassungen prüfen|anstossen, die am meisten Zeit brauchen
    - Fälle, in denen sich eine fehlende Bearbeitungsgrundlage nicht "heilen" lässt und sich geschäftliche oder technische Einschränkungen aufdrängen
    - Erfüllung Betroffenenrechte (IT-Systeme, Geschäftsprozesse)

Homburger

Vorgehensweise 2|2

- **Drei separate Tracks**
  - **Einzelne Datenbearbeitungen**
    - Sachverhalt erheben, um Anpassungsbedarf zu evaluieren
    - Bestehende Daten vs. künftig zu erhebenden Daten
    - Einstieg i.d.R. über Anwendungen (IT), nicht Geschäftsprozesse
    - Risikobasierte Entscheide über Vornahme von Anpassungen
    - Massnahmenpaket (Information, Einwilligungen, Verträge, Prozesse, etc.)
  - **Datensicherheit**
    - Wird oft in gutem Zustand sein; Handlungsbedarf ggf. betr. Data Breaches
  - **Datenschutz-Governance**
    - Sachverhalt erheben, um Anpassungsbedarf zu evaluieren
    - Massnahmenpaket (Richtlinien, Verträge, Prozesse, Training, Audit, etc.)
    - Monitoring und Dokumentation der beiden ersten Tracks

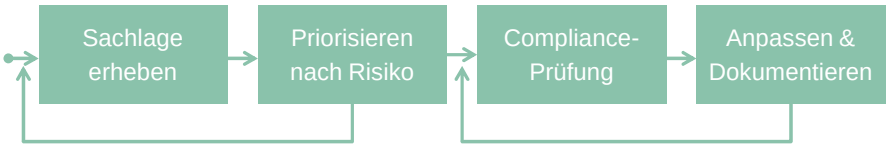
Homburger

Erhebung der Bearbeitungen

- Sachverhalt pro **IT-Anwendung** oder pro **Geschäftsprozess** erheben
  - Wer ist für eine Anwendung bzw. Bearbeitung verantwortlich?
  - Welche Daten werden wie erhoben und für welchen Zweck wie lange bearbeitet und wem auf welcher Basis gegeben?
  - Auf welcher Grundlage (Einwilligung, Gesetz, …) erfolgt die Bearbeitung?
  - Wie werden Betroffene bisher informiert?
  - Erfolgt eine Übermittlung ins Ausland und wenn ja, auf welcher Basis?
  - Welche internen Weisungen und Prozesse bestehen zum Datenschutz?
  - Besteht ein Outsourcing und wie ist es ausgestaltet ? Verträge?
  - Welches Profiling oder sonst automatisierte Einzelfallentscheide finden statt?
  - Inwieweit können Betroffenenrechte erfüllt werden? Wie hoch ist das Risiko?
  - Welches ist das Risiko eines Data Breaches?
  - Welches Datenschutzrisiko birgt die Bearbeitung für das Unternehmen?

Homburger

Gestaffeltes Vorgehen



Schritt 1: Welche Bearbeitungen gibt es? Welches Risiko bergen sie?	Schritt 2: Auswahl der Bearbeitungen, die prioritär auf Compliance geprüft werden	Schritt 4a: Prüfen, ob benutzte IT-Systeme tauglich sind	Schritt 4b: Systeme anpassen
Schritt 3: Für jede Bearbeitung den für die Compliance-Prüfung benötigten Sachverhalt erheben		Schritt 5a: Prüfen, ob Bearbeitung materiell erlaubt ist	Schritt 5b: Nötige Anpassungen vornehmen
		Schritt 6a: Prüfen, ob Bearbeitung formell konform ist	Schritt 6b: Nötige formelle Anforderungen erfüllen

Homburger

Erhebung der Governance

- Sachverhalt auf **Konzern- bzw. Unternehmensebene** erheben
  - Gibt es betriebliche Datenschutzbeauftragte oder -ansprechpersonen?
  - Gibt es ein Verzeichnis der Datenbearbeitungen?
  - Wie ist der Datenschutz in bestehenden Verträgen geregelt? IGDTA?
  - Auf welchem Stand befindet sich die technische Datensicherheit?
  - Auf welchem Stand befinden sich die organisatorischen Massnahmen zur Sicherstellung des Datenschutz (Weisungen, Trainings, Inspektionen)?
  - Gibt es einen Prozess für Verträge mit Auftragsverarbeitern? Templates?
  - Gibt es einen Prozess für die Beurteilung neuer Datenbearbeitungen?
  - Gibt es einen Prozess zur Beurteilung von Einwilligungserklärungen?
  - Gibt es einen Prozess zur Beantwortung von Anträgen Betroffener?
  - Gibt es einen Prozess für den Fall eines Data Breaches?
  - Gibt es einen Prozess zur Kontrolle der eigenen Datenbearbeitungen?

Homburger

Genereller Handlungsbedarf

- Schaffung einer betrieblichen **Datenschutzstelle** (Kompetenzzentrum)
- Datenbearbeitungen und Compliance-Massnahmen sind zu **dokumentieren**
- **Datenschutzerklärungen** (intern, extern), Verträge mit Kunden und sonstige Informationen müssen geprüft und Handlungsoptionen bestimmt werden
- **Einwilligungserklärungen** müssen geprüft und (pro futuro) angepasst werden
- **Verträge mit Providern** (und Templates) müssen geprüft und angepasst werden
- Prozesse und Richtlinien für **Betroffenenrechte** müssen etabliert werden
- Prozesse zur **Prüfung neuer Datenbearbeitungen** sind vorzusehen; Richtlinien für "Privacy by Design" und "Privacy by Default" sind zu definieren
- **Datentransfervereinbarungen** mit Konzerngesellschaften und Partnern sind zu prüfen und anzupassen bzw. abzuschliessen, falls sie noch fehlen
- Technische und organisatorische **Sicherheitsmassnahmen** sind zu prüfen und anzupassen; Prozess für den Fall von **Datenschutzverstössen** ist vorzusehen
- Prüfung der Bezeichnung eines **Vertreters** gemäss Art. 27 DSGVO

Homburger

Rollen und Ressourcen

- **Projektleitung**
  - Normalerweise Legal & Compliance als *2nd Line of Defense*
  - Ressourcen: Datenschutzspezialist (vorzugsweise intern, oder Aufbau eines internen Spezialisten mit externer Hilfe), Junior|Paralegal (intern oder extern)
- **Team "Erhebung"**
  - Erhebt den Sachverhalt im Betrieb
  - Ressourcen: Junior|Paralegal (intern oder extern) mit interner Anlaufstelle und Datenschutzspezialist (intern oder extern) für Risikobeurteilungen
- **Team "Massnahmen"**
  - Erarbeitet die nötigen Massnahmen betr. Anwendungen, Prozesse, etc.
  - Ressourcen: Vertreter aus IT, IS, Business und Legal & Compliance sowie Datenschutzspezialist (intern oder extern) als Berater betr. DSGVO
- **Management** trifft Umsetzungs- und Risikoentscheide und hält Oberaufsicht

Homburger

Schlussgedanken

- Die DSGVO wird **weniger heiss gegessen, als sie gekocht wurde**
  - Erfahrungen mit den EU-Musterklauseln und dem "Safe-Harbor"-Entscheid
  - Administrativsanktionen sind nicht das Mass aller Dinge
  - Aber: Unklare Regeln verschärfen das Risiko eines "Race to the Top"
- Trotzdem bietet heutige **Aufmerksamkeit des Top-Managements** die enorme Chance, die Datenschutz-Governance im Betrieb um Welten zu verbessern
  - Auch wenn sich in materieller Hinsicht oft nicht viel ändern wird, ungeachtet neuer Schlagworte wie "Datensparsamkeit" oder "Privacy-by-Design"
  - Datenschutz hat immerhin das Potenzial, einen ähnlichen Stellenwert in der internen Compliance zu erhalten wie das Kartellrecht (kostet aber mehr)
- **Risikobasierter Ansatz** ist zwingend, aber ohne ein Verständnis der eigenen Datenbearbeitungen und dem Treffen von Risikoentscheiden geht es nicht
  - Externe Unterstützung hilft, aber ohne interne Ressourcen geht es auch nicht

Homburger

Danke für Ihre Aufmerksamkeit.

David Rosenthal
david.rosenthal@homburger.ch
T +41 43 222 16 69

Homburger AG
Prime Tower
Hardstrasse 201 | CH-8005 Zürich
Postfach 314 | CH-8037 Zürich

www.homburger.ch

Diese Präsentation, eine Englisch-Deutsche-Ausgabe der DSGVO und weitere nützliche Unterlagen erhalten Sie unter http://www.homburger.ch/dataprotection

P764952v1