PRIVACY & LAW FS 25

GDPR

(GENERAL DATA PROTECTION REGULATION)

TOPICS

- GDPR seen from the Swiss side
- What to do - Step by Step
- Revision of the Swiss Private Data Protection Law
- Your Take Away…

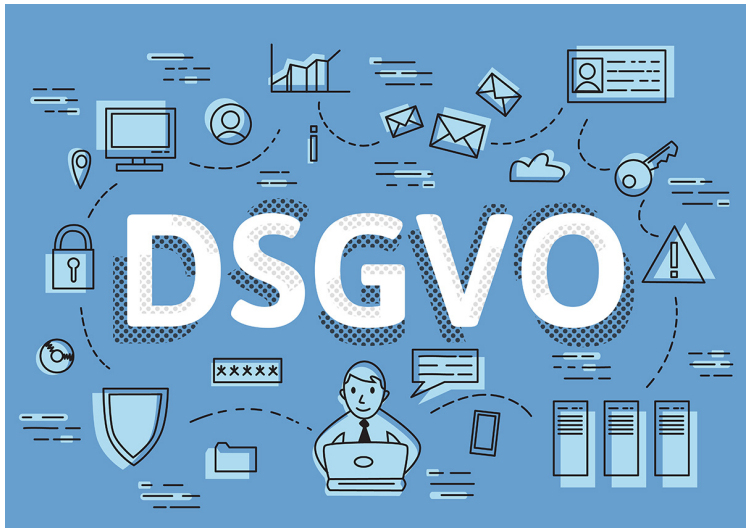
LEARNINGS

- You can independently decide whether for a Swiss company the GDPR is applicable or not,
- You know the main principles of the GDPR,
- You know the relevant steps in GDPR-projects

Heidiland, data protection & GDPR…

…true in the past, but with the 2023 revised Swiss DSG no more…

&



GDPR seen from the SWISS side (1)

Since end of **May 2018** the GDPR is **directly** for Swiss companies applicable, if:

- **they offer products and services in the EU/EWR (naming the prize in € is sufficient !) and for that they handle personal data (i.e. address, profiles etc.). Principle of the trading place: Art. 3 Abs. 2 GDPR,** or
- **they collect and exploit the personal data of website visitors from the EU (tracking by cookies, profiling with tools as Google Analytics, Facebook Pixel etc.),** or
- **they send regularly newsletter to recipients in the EU,** or
- **they handle in Switzerland by order of or as concern or part of an in the EU domiciled company personal data.**

IF ONE OF THESE CASES IS APPLICABLE, THEN THE GDPR is applicable!

tip: DSAT.ch (DatenschutzSelfAssessmentTool)

GDPR seen from the SWISS side (2)

- Generally GDPR represents only the standardised European data protection law with the goal to enforce the existing (also in Switzerland existing) principles!
- To enforce the regulation the EU-supervisory authorities have the power to proceed inspections and request for information, give orders and - in cases of severe disregard of the GDPR - **fines up to € 10-20 Mio. or up to 2-4% of the worldwide yearly turnover!**
  Check: enforcementtracker.com
- The measures have to be proportionate and effective. The possible „punishment" of Swiss companies is still unclear. Since 2017 there are no direct sanctions to a Swiss company known.
- **GDPR is only a „minimum standard"!** EU-countries may decree further and more strict regulations (i.e. § 26 german BDSG about data-processing on the work-place)!
- **We had to replace our outdated DSG 2023 with the revised one, otherwise we would have been denied the adequacy resolution (Art. 45 GDPR - secure cross boarder data transfer).**

Main difference

- Despite the wording of the GDPR looks similar to the revised CH-Dataprotection Law there's a fundamental difference: **Art. 6 GDPR!**

Processing shall be lawful only if and to the extent that at least one of the following applies:

1. **the data subject has given consent to the processing of his or her personal data for one or more specific purposes;**
2. **processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;**
3. **processing is necessary for compliance with a legal obligation to which the controller is subject;**
4. **processing is necessary in order to protect the vital interests of the data subject or of another natural person;**
5. **processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;**
6. **processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.**

   Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

- **Compare that with Art. 30 & 31 revDSG!**
- Do you recognise the similarity with our Art. 28 CC (ZGB)?

GDPR in details (1) – the revDSG is now on the same level (again)!

- **Augmenting of the peoples rights** (Art. 5/6 GDPR).
- **Data storing only as long as it is necessary** (storage limitation, Art. 5 GDPR).
- **Data protection by design and by default** (Art. 25 GDPR).
- **Big Data: Duty to Data protections impact assessment** (Art. 35 GDPR).
- **Duty to Notification of a personal data breach to the supervisory authority** (Art. 33 GDPR) **and directly to the data subject in cases of a high risk of vital violation** (Art. 34 GDPR).
- **Designation of a data protection officer** (Art. 37 GDPR). **And - if the requirements are given - a representative in the EU.** (Art. 27 Abs. 1 DSGVO).

GDPR in details (2) – the revDSG is now is now on the same level (again)!

- **When the processing is to be carried out on behalf of a controller: Only with sufficient guarantees (= contract**) (Art. 28 Abs. 1 GDPR).
- **Right to data portability in a structured, commonly used and machine-readable format** (Art. 20 GDPR).
- **Responsibility of the controller and duty to implement and document appropriate technical and organisational measures** (Art. 24 GDPR)
- **No sub-sub-processing without written consent of the responsible** (Art. 28 Abs. 2 GDPR).

WHAT TO DO – STEP BY STEP (1)

- **Base of any data protection audit is to assess the actual situation:**
  Which personal data do exist? In which form and where? For what reason? Who is responsible? Who has access? How long will be the data stored? How are they protected technically and organisationally? What are estimated the possible risks of a data breach and their consequences?
- **The GDPR requires to adapt existing contracts (i.e. consent), declarations (terms of use) and proceedings. Companies have an augmented duty to document!**
- **Appointing and naming a Data Protection Officer („DPO" - responsible) and - for Swiss companies - a representative located in the EU (= contact point for concerned persons and the authorities, Art. 27 GDPR) is necessary!**

WHAT TO DO – STEP BY STEP (2)

DSGVO-Grundlage	Aufgabe	Verantwortl.	Stand	Bemerkungen
DSGVO	Information der Führungskräfte über die bevorstehenden Änderungen			
Art. 30 Abs. 1	Relevante Verfahren zusammentragen			
Art. 30 Abs. 1	Benennung Verarbeitungsverantwortliche & Stellvertreter			
Art. 30 Abs. 1	Erstellung **Verarbeitungsverzeichnis** durch den Verarbeitungsverantwortlichen			
Art. 30 Abs. 1	Relevante **TOMs** (Technische und Organisatorische Massnahmen) für Verarbeitung zusammentragen			
Art. 30 Abs. 2	Auftragsverarbeiter über ihre Pflicht zur Verzeichnisführung unterrichten			
Art. 30 Abs. 2	Auftragsverarbeiter zur Übermittlung ihrer Verzeichnisse auffordern			
Art. 32 Abs. 1 Pkt. A	**Dokumentation Verschlüsselung** personenbezogene Daten			
Art. 32 Abs. 1 Pkt. B	**Dokumentation Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste mit dauerhaften Verfahren**			
Art. 32 Abs. 1 Pkt. C	**Dokumentation Backup**, sowie rasche Wiederherstellbarkeit			
Art. 32 Abs. 1 Pkt. D	**Dokumentation der regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs**			
Art. 32 Abs. 2	Analyse und Beurteilung des angemessenen Schutzniveaus der einzelnen Datenverarbeitungen (Vertraulichkeit, Integrität, Verfügbarkeit, regelmässige Überprüfung)			
Art. 32 Abs. 4	Nachweisführung, dass Mitarbeiter, die personenbezogene Daten verarbeiten, dies jeweils nur auf und nach Anweisung des Datenverarbeitungsverantwortlichen tun			
Art. 33	Einrichten eines Meldeweges und von Meldekriterien von Datenschutzverletzungen bei der Aufsichtsbehörde			
Art. 34	Planung des Vorgehens zur Meldung von Datenschutzverstössen an die Betroffenen			
Art. 35 Abs. 1 & 3	Schriftliche Beurteilung aller Verfahren, ob eine Folgeabschätzung notwendig ist			
Art. 35 Abs. 7	Durchführung der Folgeabschätzungen			
Art. 36 Abs. 1	Evtl. Konsultation der Aufsichtsbehörde zur Genehmigung der risikoreichen Datenverarbeitung basierend auf der Folgeabschätzung			
Art. 13 Abs. 1	Zusammenstellung einer Übersicht der datenerhebenden Dokumente und digitalen Erhebungen			
Art. 13 Abs. 1	Texte zur Erfüllung der Informationspflichten für die Erhebungen erstellen			
Art. 13 Abs. 2	Planung der Bereitstellung der in Abs. 2 genannten Informationen für alle Betroffenen			
Art. 14	Prüfung, ob Daten existieren, die nicht vom Betroffenen erhoben wurden			
Art. 14	Texte zur Erfüllung der Informationspflichten für den Datenbesitz erstellen			
Art. 24 Abs. 1	Nachweisführung der Umsetzung der TOMs durch den jeweiligen Datenverarbeitungs-Verantwortlichen			
Art. 24 Abs. 1	Verfahren zur regelmässigen Nachweisführung der Umsetzung der TOMs durch den jeweiligen Datenverarbeitungs-Verantwortlichen			
Art 24 Abs. 2	Erstellung einer **Datenschutzrichtlinie** zum Nachweis gegenüber der Aufsichtsbehörde			
Art 24 Abs. 2	**Dokumentation der regelmässigen Kontrolle der Einhaltung der Datenschutzrichtlinie zum Nachweis gegenüber der Aufsichtsbehörde**			
Art. 25	**Dokumentation von Privacy by Default und Design** durch den Datenverarbeitungs-Verantwortlichen			
Art. 4 Abs. 1 i.V.m. Erwägungsgrund 30	IP-Adresse und Cookies müssen als personenbezogene Daten behandelt werden. Anpassung der Datenverarbeitung.			
Art. 7 & 8	Anpassung der Einwilligungstexte und der Form der Einwilligung			
Art. 6 Abs. 1 Pkt. F	Nachweis der berechtigten Interessen für die Datenverarbeitung, die deren rechtliche Grundlage bildet			
Art. 28 Abs. 1	Nachweis der sorgfältigen Auswahl für alle Auftragsverarbeiter erstellen			
Art. 28 Abs. 3	**Verträge und Kontrollen mit den Auftragsverarbeitern** an die geforderten Inhalte von Abs. 3 anpassen			
Art. 28 Abs. 4 i.V.m. Abs. 1	**Nachweise der Vertragsabschlüsse mit Subauftragnehmern** von den Auftragnehmern einfordern			
Art. 39 Abs. 1 Pkt. B	Sensibilisierung der Mitarbeiter			
Art. 39 Abs. 1 Pkt. B	Schulung der Mitarbeiter über die neuen Inhalte			
	Anpassung bereits vorhandener Betriebsvereinbarungen und Arbeitsanweisungen			

WHAT TO DO – STEP BY STEP (3)

- TOM = Technical & Operational Measures
- Deep documentation of our data systems and its organisation.

Dokumentation TOM

Technische und organisatorische Massnahmen (TOM) für Verantwortliche

Der Verantwortliche bestätigt Massnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung ergriffen zu haben (Art. 32 DSGVO).

Dies sind folgende:

1. Vertraulichkeit	
1.1 Zutrittskontrolle Bauliche, technische oder organisatorische Massnahmen also z.B. Türsicherung, Sicherung des Serverraums etc.	☐ erfüllt
1.2 Zugangskontrolle Art und Stärke der Zugangsmedien sowie Aufbewahrung und Vernichtung von Informationen und Informationsträger, also z.B. Kennwortschutz etc.	☐ erfüllt
1.3 Zugangskontrolle Art und Stärke der Zugangsmedien sowie Aufbewahrung und Vernichtung von Informationen und Informationsträger, also z.B. Kennwortschutz etc.	☐ erfüllt
1.4 Trennungskontrolle Trennung der Verarbeitung, Beachtung der Zweckbindung z. B. bei Einwilligung zur Speicherung im Rahmen des Mandats, keine Verwendung für Werbung etc.	☐ erfüllt
1.5 Pseudonymisierung z.B. Daten sind ohne weitere getrennt gespeicherte Informationen nicht mehr einer natürlichen Person zuordenbar.	☐ erfüllt
2. Integrität	
2.1 Weitergabekontrolle Alle Sicherheitsvorkehrungen bei der Datenübertragung und beim Datentransport z.B. Verschlüsselungsmassnahmen etc.	☐ erfüllt
2.2 Eingabekontrolle Nachvollziehbarkeit der Datenzugriffe oder Veränderungen z. B. durch Protokollierung	☐ erfüllt
2.3 Auftragskontrolle Massnahmen bei der Auftragsdatenverarbeitung oder beim Outsourcing von Aufgaben innerhalb der Datenverarbeitung, z.B. Verarbeitung nach Art. 28 DSGVO, sorgfältige Auswahl der Vertragspartner etc.	☐ erfüllt
3. Verfügbarkeit und Belastbarkeit	
3.1 Backupverfahren Datensicherungskonzept, Wiederherstellung etc.	☐ erfüllt
3.2 Business Continuity Management Massnahmen, um in Notfallsituationen oder Störfällen angemessen, zeitnah reagierung zu können, um die Wahrung und Verfügbarkeit der Informationen sicherzustellen	☐ erfüllt
4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung	
4.1 Auftragskontrolle Regelmässige Kontrolle der Auftragnehmer	☐ erfüllt
4.2 Mitarbeiterschulung Darlegung der Schulung der Mitarbeiter in Fragen des Datenschutzes und der Geheimhaltung, z. B. auch CleanDesk etc.	☐ erfüllt
4.3 Prüfung Prozesse und Systeme sowie evtl. Zertifizierung Regelmässige Überprüfung aller Prozesse und Systeme auf Qualität und Sicherheit	☑ erfüllt

COOKIES...

- The European Court of Justice (ECJ) clearly decided on 1. October 2019 that **explicit consent** ("cookie opt-ins") **is required for cookies**.! The website operator is **obliged to provide evidence!**
  Therefore cookies should no longer be used without the user's express consent (ECJ, 1.10.2019 - C-673/17 „planet49").
- Legal base is not the GDPR but the „Richtlinie 2009/136/EG" („ePrivacy Directive")!
- Be careful: no „nudging"! (let the user decide...)
- There's a new „EU-ePrivacy Regulation" (for electronic communication) in discussion.
- Which cookies run on my site? Test with www.cookiebot.com/ (commercial service)

Is the GDPR a drawback for innovation?

- Yes & No! Innovation is still possible but it requires more legal and technical attention! (April 23: Italy's data protection authority temporally banned ChatGPD - this decision attracts EU privacy (and AI) regulators)
- Chances for new privacy- and data protection-compliant technologies and services!
- SMEs (small and medium-sized companies) struggle with legal, organisational and technical demands. Big's (FB, Google etc.) have an advantage.
- One of the winners are therefore cloud-services („hyper scalers" i.e. AWS, Google, MS, IBM), because the can easier manage the systems than a small company!

MY TAKE AWAY . . .

- . . .
- . . .
- . . .
- . . .

EXAMPLE 1

- The Business & residential promotion of the Canton Obwalden want to send regularly newsletters to interested people and companies in the EU.
- What are the legal implications?

EXAMPLE 2

- A Swiss metal-construction company is the daughter of a bigger german company. The german mother provide some central administrative services.
- Must be the Swiss customers informed that their data will be proceeded in Germany?
- Must be the Swiss customers informed about the data processor of the german mother?

EXAMPLE 3

- The Swiss Hike'n'Fly-event fly-swissalps.ch uses the german newsletter-service Brevo to inform the participants from Switzerland and abroad.
- Must a sport event also comply with the data protection law?
- Which data protection law is applicable?
- Is it sufficient to refer to the data protection rules of Brevo (Sendinblue GmbH)?