General Data Protection Regulation

Summary of
Most Relevant Business Impact

by Hauser Partners Law Firm
www.hauserpartners.ch

HP
law firm

Application of GDPR

- based Art. 7 and Art. 8 of Charter of Fundamental Rights of the European Union («CFR»)
- after 4 years of negotiations in force since May, 24 2016
- two years deadline for businesses to adjust their operations
- EU Directive 95/46 will expire on May 25, 2018
- Member State DP laws will become obsolete
- Adequacy Decisions of EU Commission and EU Standard Model Clauses remain in effect
- indirect effect on Swiss data protection legislation currently under review – Swiss Department of Justice draft regulation expected in August 2016

HHP law firm

GDPR: Constitutional Foundation

Article 7 CFR

Respect for private and family life (Recht auf den Schutz der Privatsphäre und des Familienlebens)

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 CFR

Protection of personal data (Recht auf informationelle Selbstbestimmung)

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

HHP law firm

Application of GDPR

- processing of PD basically prohibited if not explicitly allowed in the GDPR
- household exemption for private activities (e.g. private contact lists, social media)

Art. 2 GDPR

- on personal data of data subjects who are in the Union processed by
- a controller or processor with
- an establishment in the Union («Einrichtung»)

Art. 3 (1) GDPR

HHP law firm

Application of GDPR

- on personal data of data subjects who are in the Union («sich befinden») processed by
- a controller («Datenverantwortlicher») or processor («Auftragsverarbeiter») not established in the Union, where the processing activities are related to:
  - offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union
  - monitoring of their behaviour as far as the behaviour takes place in the EU («Tracking»)(«Profiling»)

Art. 3 (2) GDPR

HHP law firm

Application of GDPR

- «offering» of services in the EU:
  - not sufficient: access to a website / domain outside EU with contact dates
  - indications for offerings must (also) be focused on EU citizens:
    - using a specific language spoken in the EU
    - references to Union based customers or users
    - option to place orders in EURO or other currency in EU
    - delivery of goods to EU sites
    - operations of linked subcontractors in the EU

HHP law firm

In-House Data Protection Officer

- for enterprise, irrespective of its size, if core activity consists of
  - regular and systematic monitoring of data subjects
  - processing on a large scale of special categories of data (ethnic origin, religious beliefs, health etc.)

  Art. 37 (1) GDPR
  - could lead to aboliton of most existing in-house data protection officers - but GDPR entitles Member States to set up rules for additional DPO deployment

  Art. 37 (4) GDPR

EU Representative

conditions:

- services offered from outside the EU
- permanent processing of EU citizen`s personal data
- mandated in writing by data processor or data controller with PoA to represent controller / processor
- established in an EU Member State of data subjects affected by service offerings or profiling
- information and cooperation duties with supervisory authority
- fines only against controller or processor

Art. 27 GDPR

HP law firm

DATA PROCESSING PRINCIPLES

- lawfulness, fairness, transparency («Rechtmässigkeit, Treu und Glauben, Transparenz»)
- purpose limitation
- data minimisation
- accuracy
- storage (time) limitation (deletion routines) («Speicherbegrenzung»)
- integrity and confidentiality (Art. 32 GDPR) («Integrität und Vertraulichkeit»)
- accountability (of controller and processor, Art. 28 GDPR)

Art. 5 GDPR

HHP law firm

Lawfulness of Processing

if any of the following applies:

- DS`s consent for given purpose
- processing upon DS`s request required for performance of contract or entering into contract
- compliance with legal obligations («rechtl. Verpflichtung»)
- vital interest of DS or other person (natural disasters)
- task in the public interest based on EU/ Member State law
- legitimate interest of controller or third party (in relation to the reasonable expectations of privacy of DS; examples: legitimate defense against damage (video-surveillance, internet security, whistleblowing, fraud control); marketing purposes may or may not be covered by legimitate interest)

Art. 6 GDPR

Conditions for Consent

- oral, click-box, cookie – (implied) consent is enough – but must be unambiguous – and evidenced in case of request
- silent consent - i.e. by pre-set box - is not sufficient
- in case of sensitive data: explicit consent required
- clear, simple language
- if part of general terms - must be clearly distinguised from other text passages and possible to refuse consent
- DS may withdraw consent easily at any time – no retrospective effect: proc. prior to withdrawal remains legal
- «freely given consent» provision of services or contract unrelated to acceptance to processing of PD
- further processing allowed if new processing can be related to original purpose consent was given to («vereinbar»)

Privacy by Design

(Datenschutz durch «pro-aktive Technikgestaltung»)

adherence to the basic principles of Art. 5 GDPR through pro-active implementation of appropriate technical and organisational measures (e.g. pseudonymisation) – taking into account state-of-the art of technology, nature and purposes of processing, risks for DS and costs

Art. 25 (1) GDPR

HHP
law firm

Privacy by Default

(Datenschutz durch «datenschutzfreundliche Voreinstellungen»)

implementation of technical and organisational standard default set-ups for minimal PD according to GDPR principles limited to required purpose (principles of data minimisation, confidentiality – disclosure to third parties on «need-to-know» basis only, data storage limitation»)

Art. 25 (2) GDPR

HHP law firm

Extended Rights of Data Subjects

- Right to Information («Auskunftsrecht»)
  - right to know whether PD are collected on the DS (if the controller is not (anymore) in the position to identify the DS, he must inform the DS and credibly argue to that effect (Art. 12(2) GDPR) («glaubhaft machen»)
  - access to information on PD categories, recipients of PD, storage period (or criteria for duration), third country transfer and safeguards («geeignete Garantien»), automatic decision-making (if any), instruction on DS's other rights and legal remedies etc.
  - right to get a f.o.c. copy of PD processed (Art. 15 (3) GDPR) limitation: secrecy obligations and other lawful interests (e.g. IPR, data protection, IT security etc.)
  - refusal of information must be substantiated

  Art. 15 GDPR

Extended Rights of Data Subjects

- Right to Rectification (Art. 16 GDPR) («Berichtigungsrecht»)
  - includes DS`s right to complement incomplete information with a written statement which must be affixed to the PD («Gegendarstellung»)
  - controller is obliged to inform third party recipients of rectification of PD (Art. 19 GDPR) if not impossible or disproportionate («public statement»)
- Right to Erasure (to be Forgotten) (Art. 17 GDPR)

  («Löschungsrecht», «Recht auf Vergessen werden»)
  - if PD are no longer necessary for the provided purpose for processing (further processing is illegal) limit: public interest, free speech, free press)
  - DS withdraws consent for future processing («opt-out»)
  - DS objects to processing and there is no (other) legitimate purpose for it
  - DS objects to processing to direct marketing purposes incl. profiling

  «erasure» does not mandatorily mean complete deletion on all instances and data carriers but «inusability for the ordinary, intended use», e.g. permanent blocking of internet database access; in case of PD made public, controller must inform public must delete copies and links

HP law firm

Extended Rights of Data Subjects

- Right to Restriction of Processing (Art. 18 GDPR) («Recht auf Einschränkung der Verarbeitung» , «Sperrung»)
  - in case accuracy of PD is contested (as long as required to review the data by controller)
  - DS requires the PD to be restricted instead of being erased
  - DS requires the PD to be maintained but restricted on behalf of own legal interests
  - where DS objects based on Art. 21 (1) GDPR (right to object to processing for public interest or legitimate interests) - gives controller time to respond
- Right to Data Portability (Art. 19 GDPR) («Datenübertragbarkeit»)
  - only PD collected from the DS
  - processing was based on consent or on contract fulfillment
  - PD must be returned to DS or transferred directly to other controller
  - PD must be provided in a structured, commonly used, machine-readable format
- Right to Object (Art. 21 GDPR) («Widerspruchsrecht»)
  - in case of data processing in public interest, with «legitimate interest» or in case of profiling (marketing purposes) in case of direct marketing: processing must cease immediately
- Right not to be subject to automated decision-making (Art. 22 GDPR) («profiling», «scoring») Exception: for closure / perfomance of contract, consent – but with human intervention

Process Docu & Impact Assessment

- **Records of processing activities**

(«Verzeichnis von Verarbeitungstätigkeiten»)

all processing activities must be recorded

details of processor, purpose of processing, categories of personal data and data subjects, recipient categories, third country transfer details, technical and organizational security measures, time history etc. (Art. 30 GDPR)

- **Impact Assessment Duty**

(«Datenschutz – Folgenabschätzung »)

in case of high risks for data subjects, due to large scale processing of sensitive data, profiling, use of new technologies, etc.

- GDPR tightenings:
  - executive management duty –
  - applies on processors
  - documentation of impact ass.

HP law firm

Data Security Measures

- obligation on controller (and new on processor) to implement technical data security and organisational measures as well as data protection policies in order to ensure compliance with GDPR (Art. 24 GDPR)
- pseudonymisation and encryption are now general measures of technical data security
- entry-, access-, transfer- control are now included in a general confidentiality obligation of PD
- obligation to regularly monitor and review data security measures
- quality of measures relevant in case of fines following infringments of GDPR

Information Duties

- extended catalogue under the GDPR
- data protection declarations must be adjusted and complemented with the new information until end of May 2018
- GDPR differentiates between PD obtained from the DS and the PD obtained from third party (e.g. contract partner of controller)

Information Duties

- identity and contact details of controller and data protection officer, EU Rep (if any)
- purpose and legal grounds for processing (Art. 6) («Zweckverfolgung» und «Rechtsgrundlage»)
- recipients or categories of recipients (e.g. marketing partners)
- third country transfers and contractual safeguards taken, incl. access to / provision of such safeguards to DS
- data storage limitation
- on DS`s rights (information, rectification, erasure, restriction of processing, objection rights, portability etc.)

Art. 13 (1) GDPR

HHP law firm

Information Duties

- in case of DS`s consent: on right to withdraw the consent at any time
- right to lodge a complaint with supervisory authority
- nature of obligation to provide PD for collection (contractual, statutory, required for contract performance etc.)
- on automated decision making (incl. profiling) and its logic and consequences (if any)
- on intention to future processing for other purpose

Art. 13 (1), (2), (3) GDPR

HP law firm

New Information Duties

- in case of consent: DS must be informed of opt-out rights and of no retroactive effect of opt-out (withdrawal of consent)
- indication of legitimate interest
- data storage limitation
- on rights of DS
- on automated decision-making (if applicable)
- instruction of legal remedy («Beschwerderecht»)
- source of PD (if they are not obtained from DS)
- duties apply as well if PD is provided through third party (Art. 14 GDPR)

Form of Information

- in writing or electronically (orally on request of DS)
- easy accessible (e.g. on website with link)
- stand-alone data privacy statement (or distinguished in GT`s)
- clear, plain language or standardised icons
- prior or at collection of data
- in case of PD not obtained from DS: within 1 month from PD receipt and/or before disclosure to recipient
- free of charge (unless rights abuse by DS)
- upon DS`s request: without undue delay but at least within one month

Art. 12, 13, 14 GDPR

HHP law firm

Personal Data

- information relating to an identified or identifiable natural person
- directly or indirectly «identifiable» («identifizierbar»)
- e.g. by through identifiers or «quasi-identifiers», such as ID-number, location data, online identifier (IP-address, cookie) or one or more factors specific to the physical, physiological, genetic, mental, cultural or social identity of that person

Art. 4 (1) GDPR, Recital 30 to GDPR

Personal Data

- special categories of PD subject to further restrictions – «sensitive» PD

  (ethnic origin, health, political, religious views, trade union memberships, sex life and orientation, biotmetric and genetic data)

  Member States are entitled to exclude consent option to processing of sensitive data
- explicit consent of DS (vital interest, public interest etc.)
- health data: all information related to body irrespective of source (doctor's report, medical files, fitness-apps, wearables etc.)
- quantified-self and/or fitness data are health data and subject to the stricter requirements of Art. 9 GDPR
- processing of health-related PD explictly allowed for public healthcare, social welfare etc. and where professional secrecy obligations apply

Art. 9 GDPR

HHP law firm

Personal Data

- controversial definition

- relative view (business oriented view)

cookie, IP-address, pseudonym, heart rate, intelligent TV, GPS-data etc. is not a personal data per se. It may only become one depending on context, additional information or knowledge

- absolute view (data privacy oriented view)

a combination of single anonymous data can easily lead to identification – therefore each single data is considered a personal data irrespective of additional information available and of what effort would be required to get to additional information

Ex.: Federal Counsellor & shoe size / cook & Interlaken & body mass index / female & Switzerland & 44 & heart rate & height

Personal Data

- conflict is not definitely solved in the GDPR; it is still possible to de-identify PD, so that they are considered «anonymous» or «statistical» data not subject to GDPR
- Recital 26 to GDPR relies classification as a PD on whether or not an individual can be identified with reasonable effort, taken into account current technology, time efforts and related costs
- Tendency is towards a broad interpretation of PD

HHP
law firm

Personal Data

- absolute view of DP authorities leads to the conclusion that a data controller must prove to authority that identification of a single individual can virtually be excluded
- BIG DATA: data aggregation: more data accuracy but conflict with GDPR principles of data minimisation, purpose limitation and the DS`s rights (spec. to information, rectification of incorrect PD, erasure, data portability etc.)
- BIG DATA ANLYTICS algorithms are more and more able to analyze huge data pools, compare them with other (e.g.public) data pools and discover inherent, previously unknown references and information about individuals

Statements of the Swiss DP Authority on Big Data:
http://www.edoeb.admin.ch/datenschutz/00683/01169/01344/index.html

Personal Data

- state-of-the-art encrypted data
- with no key access for data controller or processor are not considered personal data and are not subject to professional secrecy (such as patient - doctor secrecy)

- processing of encrypted PD ? IaaS, SaaS ?

HHP
law firm

Personal Data

- pseudonymisation: tool used in GDPR for data security and confidentiality purposes only – not to remove qualification as «Personal Data»
- pseudonymisation still enables «singling out» of individuals and «linking» across different data sets and data pools
- legal uncertainty on degree of modification of PD required for complete, irreversible anonymisation
- technical progress requires periodic re-assessment of data quality of de-identified data pools

Anonymisation of Personal Data

- effective anonymisation must
  - prevent singling out of an individual in a data pool
  - prevent gaining information to single individuals through linking of two data sets or pools
  - prevent inferring information betw. data sets or pools
  - provide a consistent and systematic de-identification process of PD without depriving PD of its information value

Source: Article 29 Data Protection Working Party Opinion 05/2014 «on Anonymisation Techniques» 0829/14/EN WP216

HHP law firm

Anonymisation of Personal Data

- combination of quasi-identifiers such as birth date, gender, zip code, profession – leads to easy identification
- quasi-identifiers should only be used if of value for data analysis
- re-identification through re-combination of previsously separated data pools (knowledge) can be avoided through permanent deletion of one of the two pools or additional knowledge

Anonymisation of Personal Data

- «generalization»: instead of home address: city, district or country; instead of exact numbers of age, income or blood pressure: intervals (e.g. «30 - 40 years of age»).
- «randomisation»: modification of veracity of parts of the data in order to remove link to individual
- «k-anonymity»: each category of individuals with a certain (e.g. health) attribute must contain several individuals in the data pool (i.e. 3 billionaires instead of 1)
- «t-closeness»: aims to create equivalent classes that resemble the initial distribution of attributes in a pool
- «aggregation»: the more of individuals PD are included in a data pool the more difficult is singling out or referring

Codes of Conduct and Certification

- GDPR promotes the drawing up of codes of conduct and establishment of certification bodies and certification mechanisms for data protection seals and marks to voluntarily demonstrate compliance with the GDPR
- codes of conduct and certification mechanisms are open for PD controllers or processors not subject to the GDPR in order to demonstrate appropriate safeguards with third country transfers of PD

Art. 40, 41, 42 GDPR

HHP law firm

Data Processors` Duties

- controller must ensure to involve only processors providing sufficient guarantees with regard to data security (Art. 28 (1) GDPR)
- unlike the Directive, the GDPR establishes direct legal duties on data processors (e.g. the restrictions to transfer PD to third countries; o nominate a data protection officer or EU representative, to cooperate with supervisory authority, to implement technical and organisational measures; to document the processing etc.)
- additional duties must be imposed in a contract (electronic or written) or other binding act by controller on processor (e.g. obligation of processor to use only personnel subject to secrecy obligation, Art. 28 (3) lit. b)
- no direct obligation to directly respond to DS`s rights – but to support Controller in this respect

Extended Duties of Processors

- subcontractors of processors:
  - involvement or change of subcontractors by processor requires prior written authorisation by controller (Art. 28 (2) GDPR)
  - data processor must contractually be obliged to impose same legal duties on its subcontractors (Art. 28 (4) GDPR)
  - data processor remains responsible to the controller for for the fulfillment of GDPR obligations (Art. 28 (4) GDPR

Data Transfer to Third Countries

- principle of «adequacy of level of protection» still applies – but requirements for an adequacy decision by the EU Commission are higher (e.g. effective execution of data protection laws; effective judicial remedies of DS; independent supervisory authorities etc.)
- existing adequacy decisions remain in place but are subject to periodic review by Commission
- July 12, 2016: adequacy decision for «Privacy Shield» self-certify framework for US companies – in place since 1st of August 2016
- EU Standard Model Clauses and BCR remain valid tools for lawful third country PD transfer

HHP law firm

Data Transfer to Third Countries

- third country recipients are subject to binding and enforceable code of conducts or certification mechanisms (Art. 46 (2) lit. e GDPR)
- single appropriate safeguards approved by supervisory authority (e.g. single, individual contracts)
- consent of DS to the transfer (Art. 49 (1) lit. a GDPR)
- exemption catalogue (contract fulfillment, pre - contractual measures on request of DS, public interest, legal claims, vital interests etc.) (Art. 49 (1) lit. b – g GDPR)
- in case of non-repetitive transfers of limited number of DS and compelling legitimate interests of controller and notification of supervisory authority (Art. 49 (1) second sentence GDPR)

HHP law firm

Notification of Data Breach

- to supervisory authority without undue delay at least within 72 hours
- unless unlikely to result in a risk to rights and freedoms of individuals
- notification to Data Subjects without undue delay in case of risk to rights and freedoms
- unless appropriate technical measures (e.g. encryption) were taken so that risk no longer likely to materialize
- fines: 10 Mio EURO or 2% of revenue

HHP
law firm

Remedies, Liability & Sanctions

- sanctions by supervisory authority
  - monetary fines up to the higher of 10 Mio or 20 Mio EURO or 2% respectively 4% of annual ww revenue (depending on GDPR rule infringed)
  - amount depends on severity of infringement, impact of data leak, sensitivity of personal data involved, risk to individuals

  Art. 83 GDPR

  Member States may issue additional penal sanctions

  Art. 84 GDPR

HHP law firm

Remedies, Liability & Sanctions

- Data Subject`s Remedies
  - right to lodge a complaint with supervisory authority
  - right to an effective judicial remedy against supervisory authority's action or non-action
  - claim for material and immaterial damage caused by infringement of GDPR against controller or processor either at the establishment of controller or processor or at the habitual residence of data subject
  - right to be representend by NGO`s
  - controller / processor: right to exculpation

Art. 77 ff. GDPR

HHP law firm

Remedies, Liability & Sanctions

- Data Controller`s or Processor`s Remedies
  - right to an effective judicial legal remedy against a decision of a supervisory authority
  - legal remedies under the procedural rules of national law against claims of data subjects, claims between data controller and data processor against decisions of national courts

Legal Notice

HauserPartners does not provide any explicit nor implied guarantee or warranty whatsoever as to the completeness or accuracy of the content of this presentation and the legal views expressed.
HauserPartners does not take any liability for damage caused by reliance on the content of this presentation.

HauserPartners
Law firm
Balsberg
CH-8058 Zurich-Airport
www.hauserpartners.ch
info@hauserpartners.ch