AmCham's HR Committee's

GDPR / Data Privacy Roundtable

19. SEPTEMBER 2017

LUNDGRENS

THE REGULATION

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

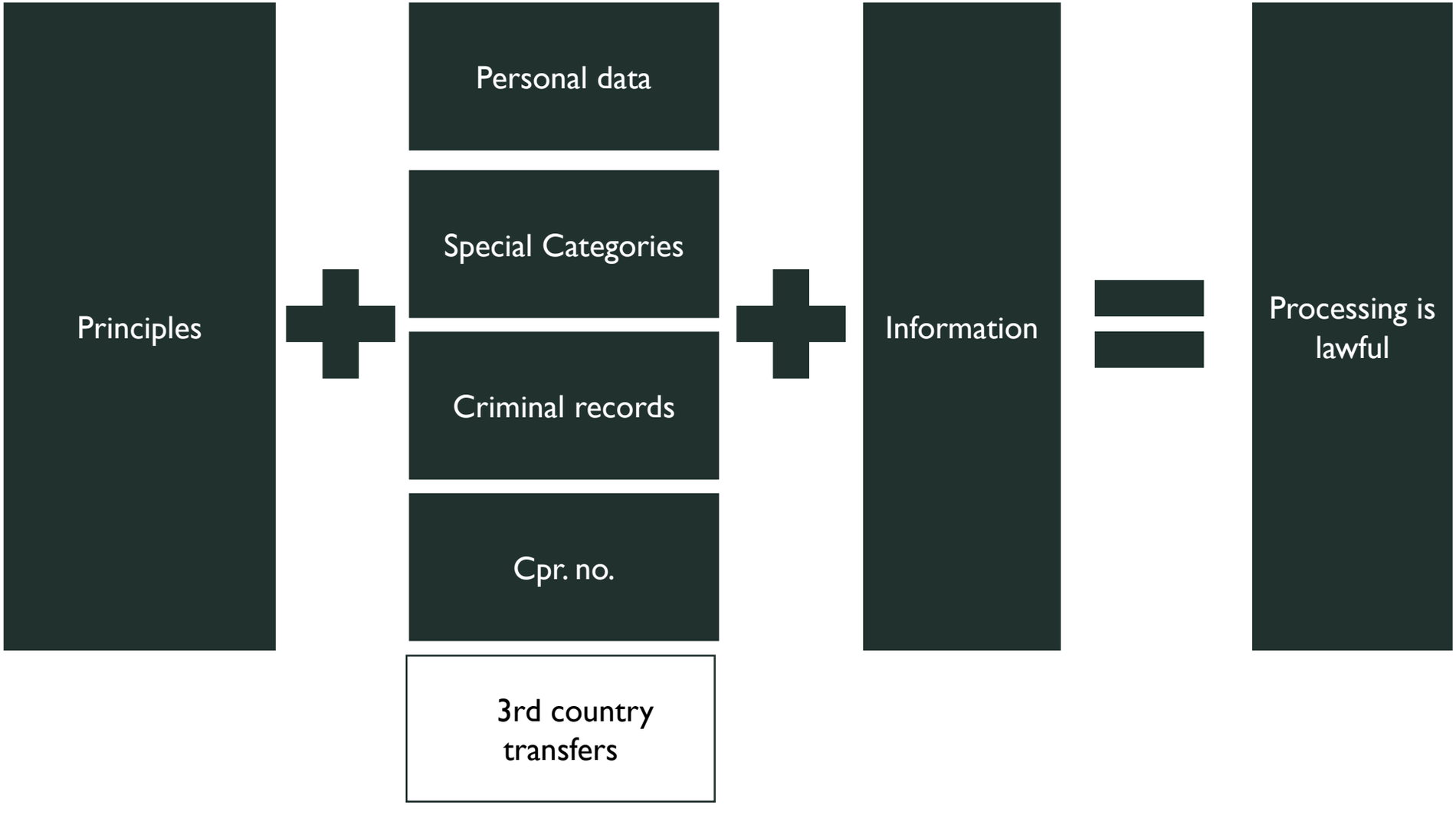
..among friends 'the GDPR'

- A Regulation
- Applicable from 25 May 2018
- Revolution or Evolution ?
- Why is data protection suddenly a hot topic?

BRIEF OVERVIEW – DATA CONTROLLER OBLIGATIONS

LUNDGRENS

LAWFULNESS OF PROCESSING



LUNDGRENS

PRINCIPLES

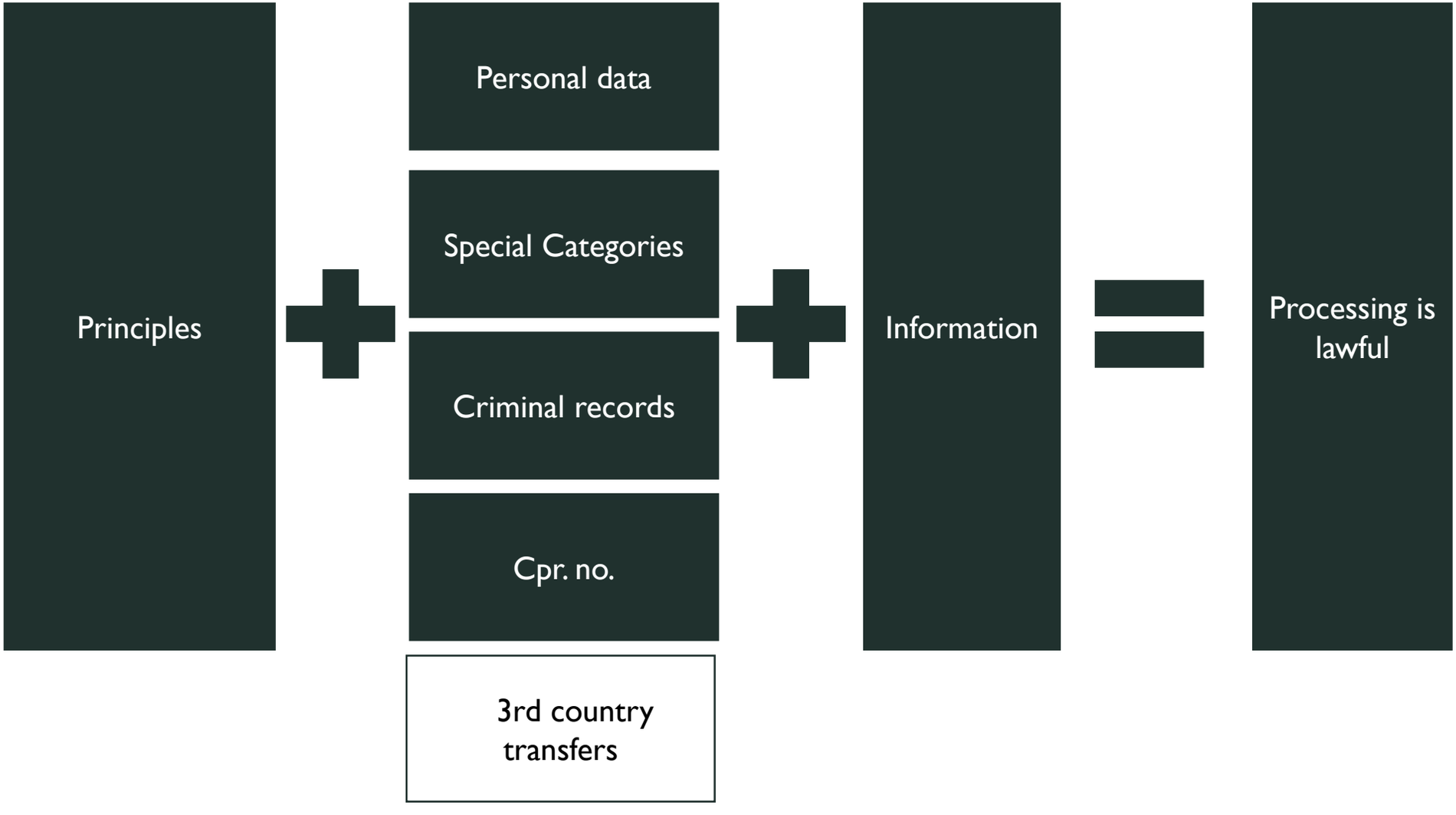
Lawfulness, fairness and transparency'	• processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	• collected for specified, explicit and legitimate purposes and • not further processed in a manner that is incompatible with those purposes
Data minimisation	• adequate, relevant and limited to what is necessary in relation to the purposes
Accuracy	• accurate and, where necessary, kept up to date
Storage limitation	• no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	• ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability	• **The controller shall be responsible for, and be able to demonstrate compliance**

LUNDGRENS

LAWFULNESS OF PROCESSING

GDPR Art 6	GDPR Art 9	GDPR Art 10	GDPR Art 87
Personal data	**Special categories**	**Criminal records**	**CPR-no**
• Name, adress, birthdate, sex etc • Application, CV, education, experience, • Responsibilities • Salary and benefits • Absence – holiday - sickness • Disciplinary measures, • relatives • Email/internet • Photo - CCTV, • Personality test List not exhaustive	• racial or ethnic origin, • political opinions, • religious or philosophical beliefs, or • trade union membership, • genetic data, biometric data • health • sex life or sexual orientation List is exhaustive	Transcript of criminal record	123456-7890
Lawful processing	**Lawful processing**	**Lawful processing**	
• consent • Necessary for performance of contract • Compliance with a legal obligation • Protect Vital interest of data subject • Balancing of interest …..and more.	• **Prohibited, except**; • Explicit consent • Rights and obligations under employment law or collective agreement • Establish, exercise or defend legal claims • Data made public by data subject ….and more	• Explicit consent	• Consent • Compliance with legal obligation

LAWFULNESS OF PROCESSING



LUNDGRENS

DATA SUBJECT RIGHTS

Information and Access	• Right to receive certain information at the time of collection – irrespective of source of collection • Ret to subsequently request information (entitled to a copy) (Art 13 -15)
Rectification	• rectification of inaccurate personal data/ right to have incomplete personal data completed (Art. 16) • communicate any rectification to each recipient to whom the personal data have been disclosed (modif: impossible/disproportionate effort. (Art 19)
Right to be forgotten	• Right to erasure – but right is not unconditional !(Art 17) • communicate any rectification to each recipient to whom the personal data have been disclosed (modif: impossible/disproportionate effort. (Art 19)
Restriction of Processing	• Right under certain conditions to have processing restricted ('freezing of processing') (Art 18) • communicate any rectification to each recipient to whom the personal data have been disclosed (modif: impossible/disproportionate effort. (Art 19(Art 19)
Data portability	• Right to receive the personal data which data subject has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller (Art 20)
Right to object	• Right to object, on grounds relating to data subjects particular situation, to processing of personal data which is based on the balancing of interest test (Art 21) – • Right to object against processing for direct marketing purposes and automated decisions (Art 22)
How to respond	• in a concise, transparent, intelligible and easily accessible form, using clear and plain language- and free • Within one month of receipt of request (Art 12) • Exceptions and limitations apply (Art 23) and supplementing national law.

GENERAL OBLIGATIONS

Accountability	• Implement, review and update appropriate technical and organisational measures to ensure and to be able to demonstrate compliance
Data Protection Policies	• Where proportionate in relation to processing activities, the measures shall include the implementation of appropriate data protection policies
Data Protection by Design	• Processing activities and products should be designed to implement data protection principles, • Eg. data minimization, pseudonymisation , integrate safeguards etc.
Data Protection by Default	• by default, only data which are necessary for each specific purpose of the processing are processed. • E.g. the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility
Responsibility for data processors	• Only use data processors that guarantee compliance and protection of privacy • Due diligence on data processor and the solution. Monitoring and audit • Must be governed by written contract
Records of Processing Activities	• Purpose, categories of data subjects, personal data and recipients, timelimits for erasure, safety measures • Exception for organisations employing fewer than 250 employees – but only if processing is only occasional
Cooperation with Supervisory Authority	• cooperate, on request, with the supervisory authority in the performance of its tasks • Notification and approval of certain processing no longer required

SECURITY OF PERSONAL DATA

Technical and organisational safety measures	• Risk based approach considering state of the art, the costs of implementation and the nature, scope, context and purposes of processing - No specific requirements but GDPR suggests to consider:
	  • Pseudonymisation and encryption of personal data
	  • ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems
	  • ability to restore the availability and access to personal data in a timely manner
	  • regularly testing, assessing and evaluating the effectiveness of safety measures

Notification of a personal data breach	• **without undue delay and not later than 72 hours after having become aware of the breach** • describe the nature of the breach including, the categories and approximate number of data subjects and data records concerned • the likely consequences of the breach and measures taken to address the breach • Be able to document the breach and the measures taken • If breach is likely to result in a high risk to data subjects, the controller shall notify the data subjects
Data Protection Impact Assessement	• If new or amended processing activities are likely to result in high risk for data privacy (e.g. new technology, large scale processing of special categories) the controller must perform a DPIA • DPIA must include description of a) the intended processing activity and the purpose, b)an assessment of the necessity and proportionality c) an assessement of the risks involved and the measures taken to address the risks • Where appropriate seek the view of the data subjects (e.g. work council) • If still a high risk – prior consultation with data protection authority
Data Protection Officer (DPO)	• advise and monitor compliance – serve as contact point for data subjects and authorities etc • core activities require regular and systematic monitoring of data subjects on a large scale; or • core activities consist of processing on a large scale of special categories of data • Independent - protected

BRIEF OVERVIEW – DATA CONTROLLER OBLIGATIONS

LUNDGRENS

LUNDGRENS TEAM

MICHAEL GORM MADSEN
ADVOKAT, PARTNER
DIR: +45 3525 2930 / MOB: +45 2524 5130
MAIL: MGM@LUNDGRENS.DK

- Specialiseret i persondataretlige spørgsmål med betydelig erfaring med juridisk og strategisk rådgivning i alle aspekter af persondataretten
- Stor indsigt i juridiske problemstillinger i relation til Internet og e-handel
- I 2013 certificeret som Information Privacy Professional CIPP/E af The International Association of Privacy Professionals (IAPP)
- Medlem af Dansk Forening for Persondataret

MAJA KRARUP
ADVOKAT
DIR: +45 3525 2935 / MOB: +45 2524 5135
MAIL: MHK@LUNDGRENS.DK

- Advokat i Lundgrens' afdeling for persondataret.
- Mange års erfaring med at rådgive danske såvel som udenlandske klienter om alle aspekter af persondataretten.
- Særlig fokus på udarbejdelse og implementering af compliance-programmer i forbindelse med EU Persondataforordningen.
- Medlem af Dansk Forening for Persondataret