KHAITAN &CO

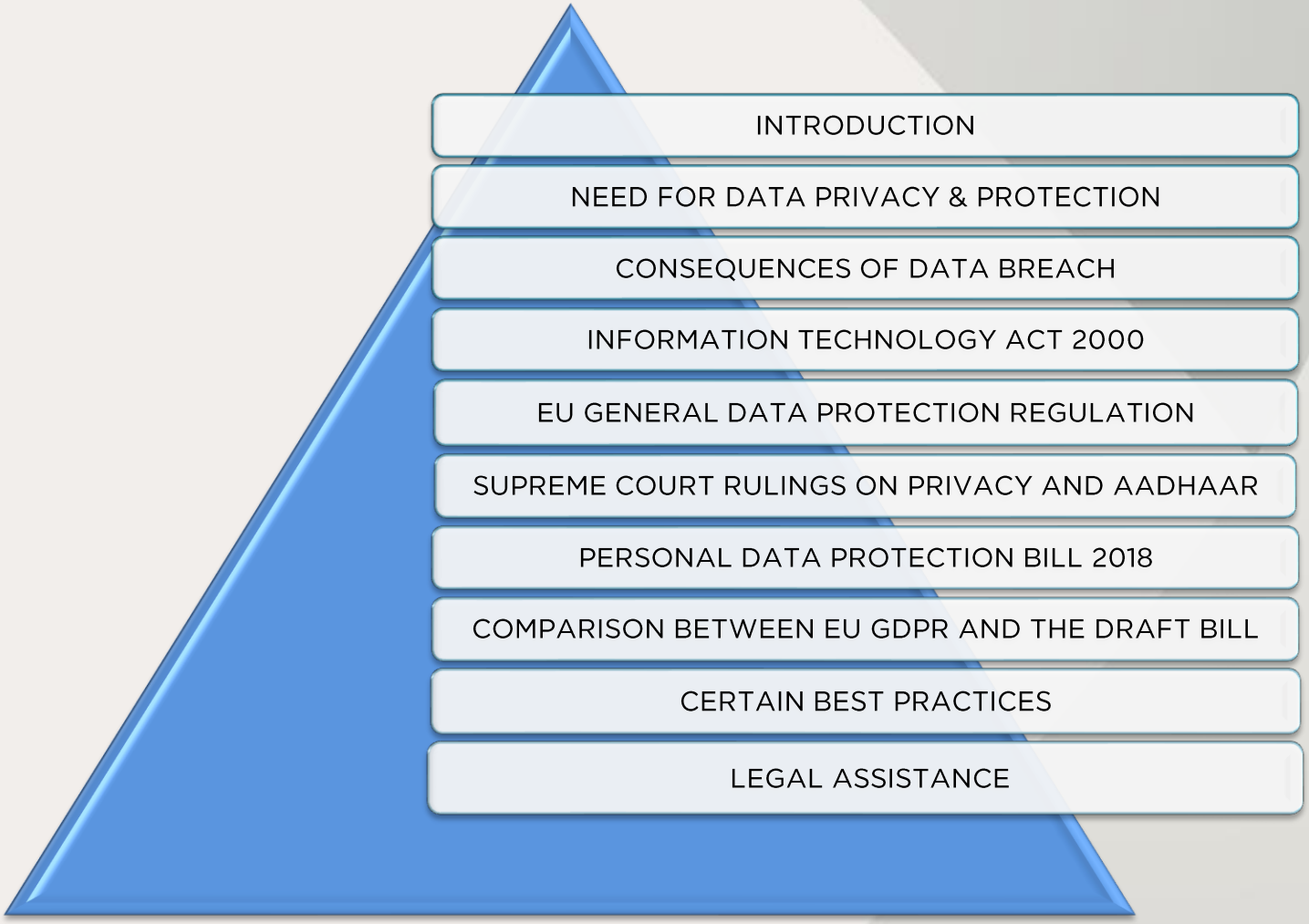
Advocates since 1911

DATA PRIVACY

Supratim Chakraborty

12 December 2018

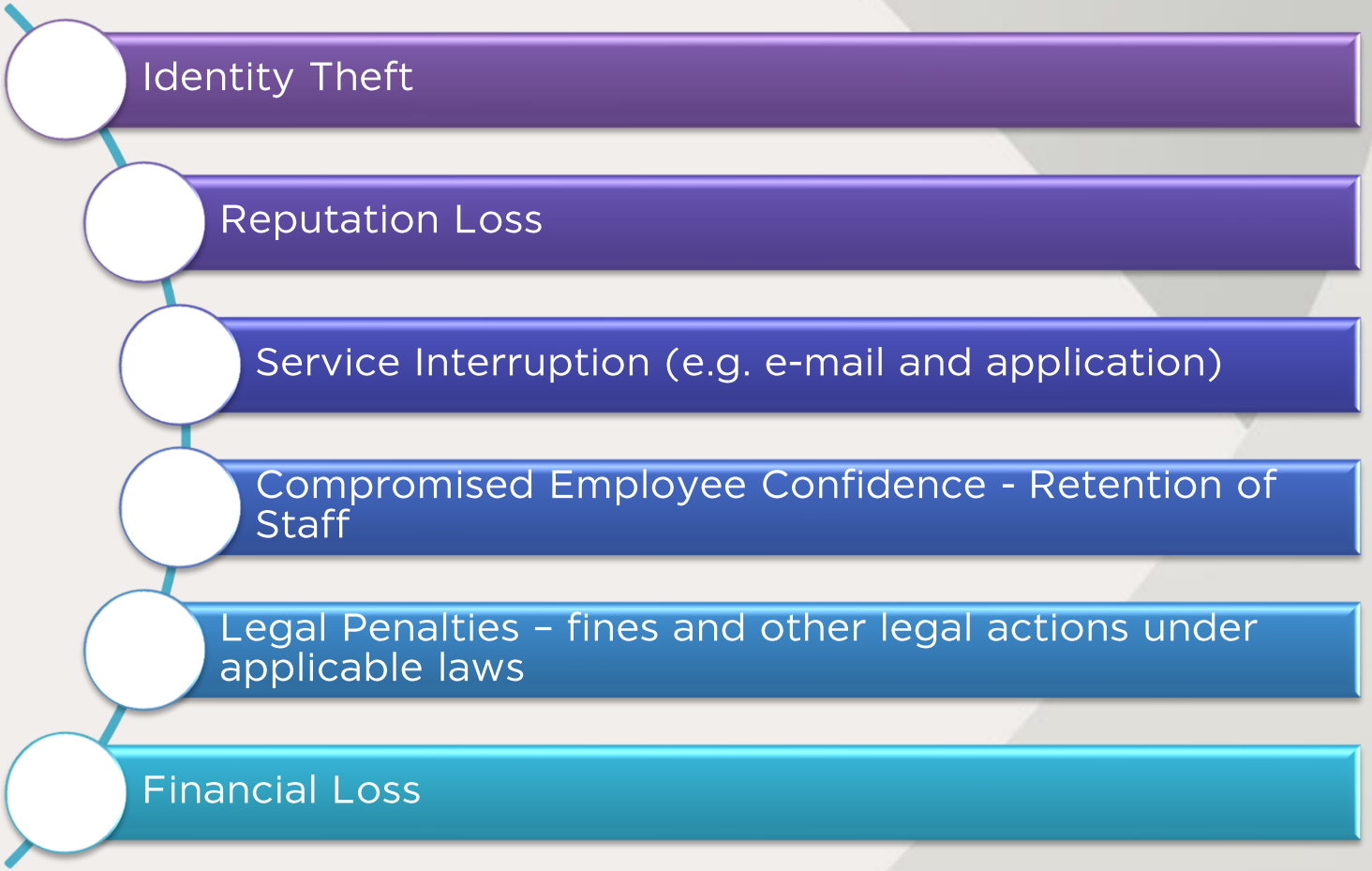
Route Map



Need for Data Privacy & Protection

- Data is corporate asset
- To protect privacy of individuals
- To prevent unauthorized usage
- Minimizing financial loss due to data loss
- Earn trust of customers and employees

Consequences of Data Breach



Present Legal Framework in India

DATA PROTECTION LAW	• No exclusive legislation
RIGHT TO PRIVACY	• Fundamental Right under Article 21 of the Indian Constitution
PRIMARY LEGISLATION	• IT Act and the IT (Reasonable Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("**Privacy Rules**")
OTHER LEGISLATIONS	• The Indian Penal Code 1860 • Sectoral regulations

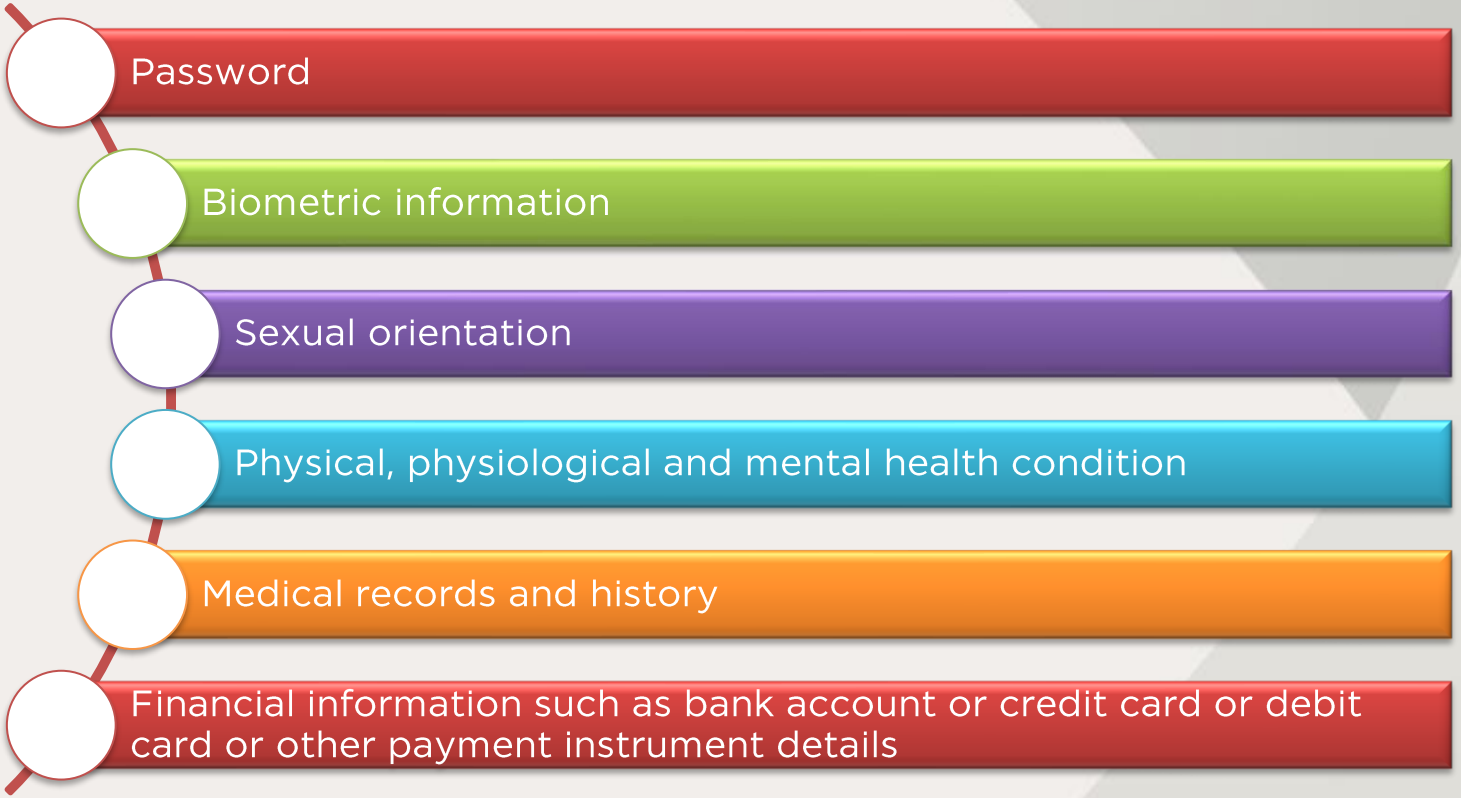
IT Act | Few Relevant Sections

- Section 43 A:
  - Relates to any body corporate possessing, dealing or handling any **sensitive personal data or information** in a computer resource
  - Where such body corporate is negligent in implementing and maintaining **reasonable security practices and procedures**
  - Causes wrongful loss or wrongful gain to any person
  - Liable to pay **damages by way of compensation** to the affected person

IT Act | Explanation To Section 43A

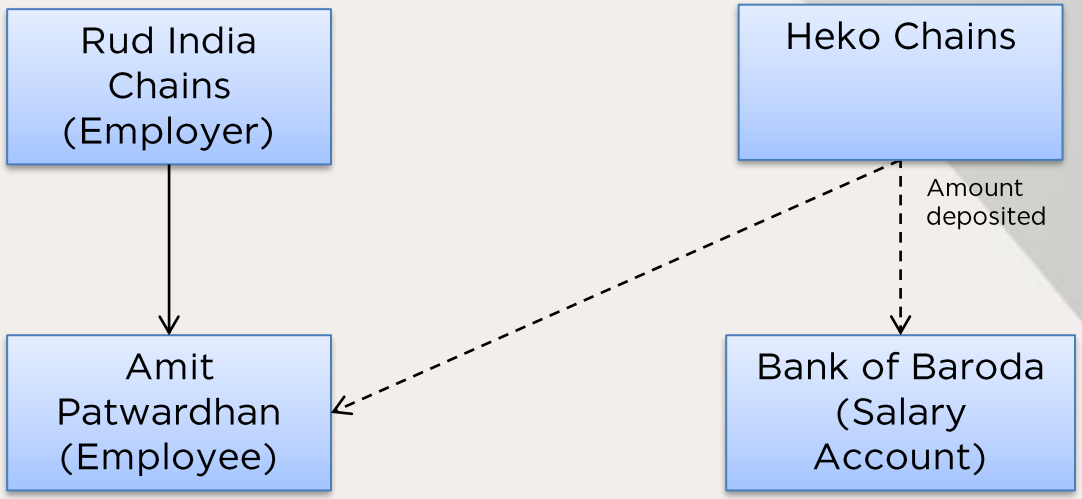
- **Reasonable Security Practices and Procedures** - security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties **or** as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit
- **Sensitive Personal Data or Information ("SPDI")** - such personal information as may be prescribed by the Central Government

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011



Personal Information: Information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person

Case Law | Amit Patwardhan v BOB



- Bank Account Statements held to be SPDI
- Amit Patwardhan not awarded any amount in the first case with his employer
- In the present case, Bank of Baroda asked to pay a token compensation of INR 5,000

Privacy Rules | Watch-Out Areas

IT Act | Few Relevant Sections

- Section 72 A:
  - Relates to any person providing **services under lawful contract** wherein personal information is accessed
  - There is intent or knowledge of wrongful loss or wrongful gain being caused through disclosure of such personal information
  - Disclosure is made **without the consent of the person** concerned **or in breach of a lawful contract**
  - Liable to be **punished with imprisonment** up to **3 years**, or with **fine** up to **INR 0.5 Million**, or with **both**

Can you identify sensitive personal data under present day Indian law?

1. Religion	2. Biometric information	3. Address
4. Medical records	5. Criminal record	6. Insurance renewal date
7. Sexual orientation	8. Name	9. Passport number
10. IP address	11. Email address	12. Password
13. Political opinion	14. Phone number	15. Bank account details

Yes

No

Does the GDPR apply to you?

GDPR | Offences and Penalties

Higher of 20M EUR or up to 4% total worldwide annual turnover in the last FY

Offences such as infringement of data principal rights and unauthorized cross border transfer of personal data to countries or organizations

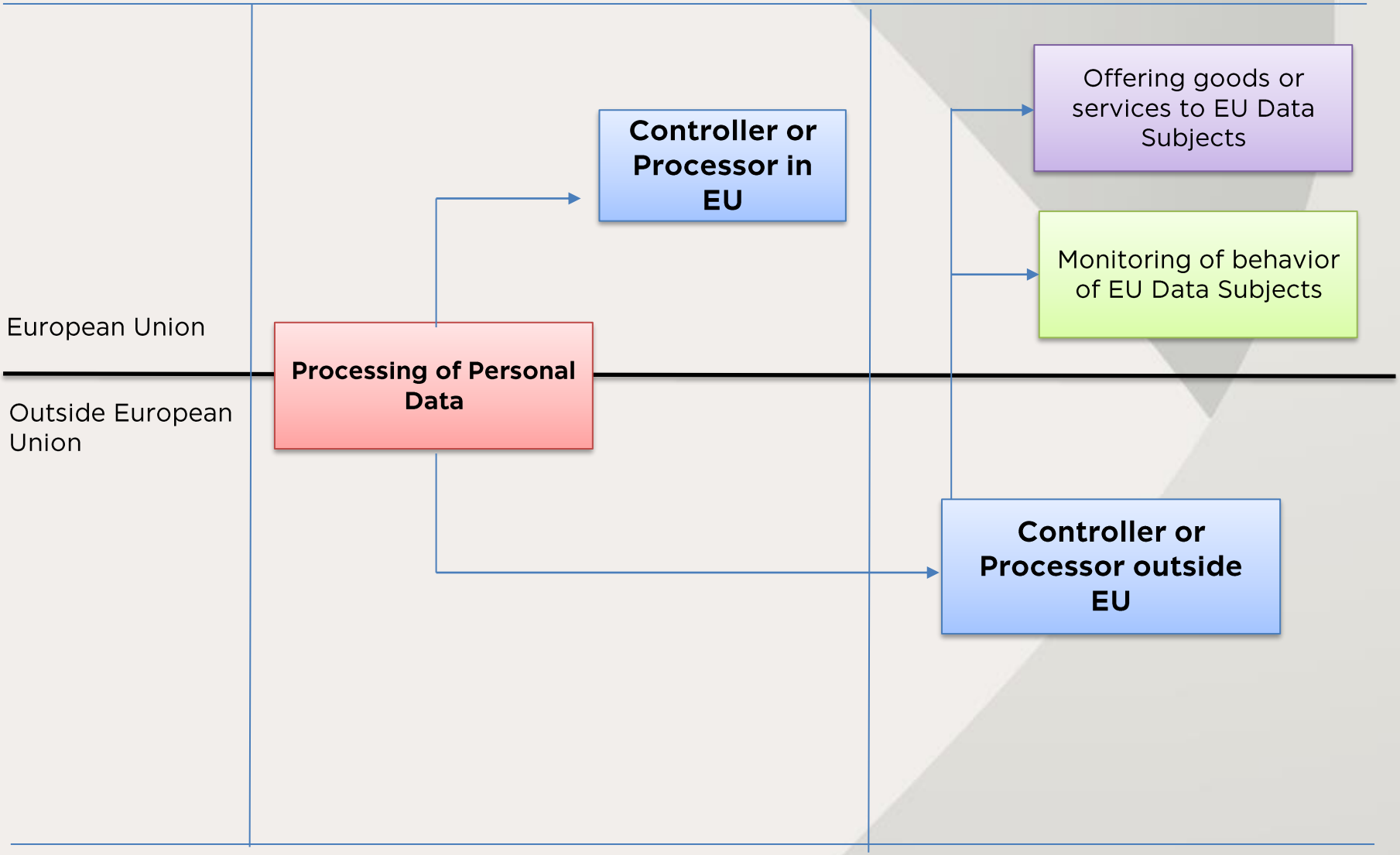
Higher of 10M EUR or up to 2% total worldwide annual turnover in the last FY

Offences such as failure to protect personal data by design and default and failure to conduct data protection impact assessment

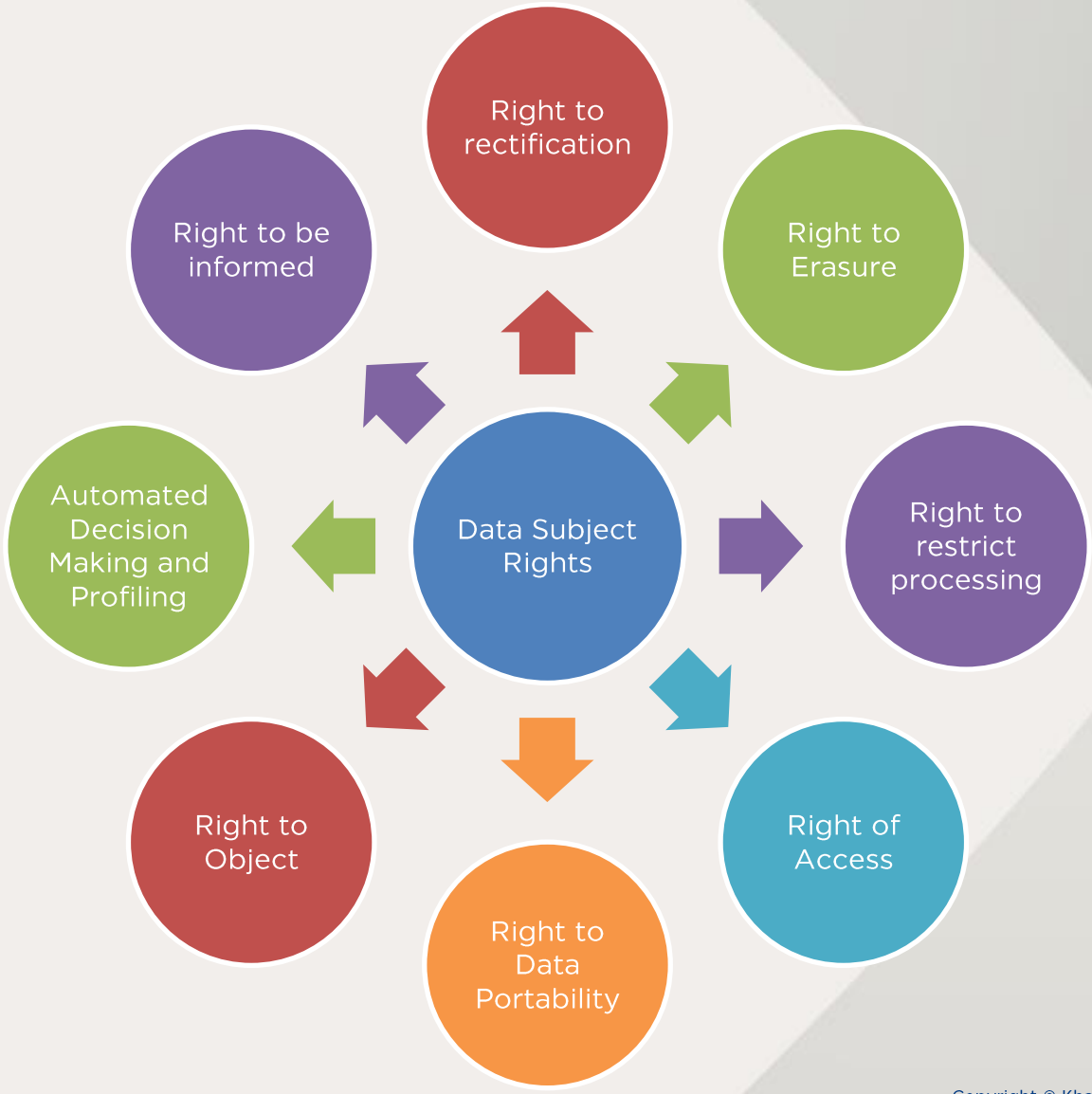
GDPR | Overview

General provisions	• Chapter 1 (Art. 1 – 4)
Principles	• Chapter 2 (Art. 5 – 11)
Rights of the data subject	•Chapter 3 (Art. 12 –23)
Controller and processor	•Chapter 4 (Art. 24 – 43)
Transfers of personal data to third countries	• Chapter 5 (Art. 44 –50)
Independent supervisory authorities	• Chapter 6 (Art. 51 – 59)
Cooperation and consistency	• Chapter 7 (Art. 60 – 76)
Remedies, liability & penalties	•Chapter 8 (Art. 77 – 84)
Specific processing situations	•Chapter 9 (Art. 85 – 91)
Final provisions	• Chapters 10/12 (Art. 92 – 99)

GDPR | Applicability



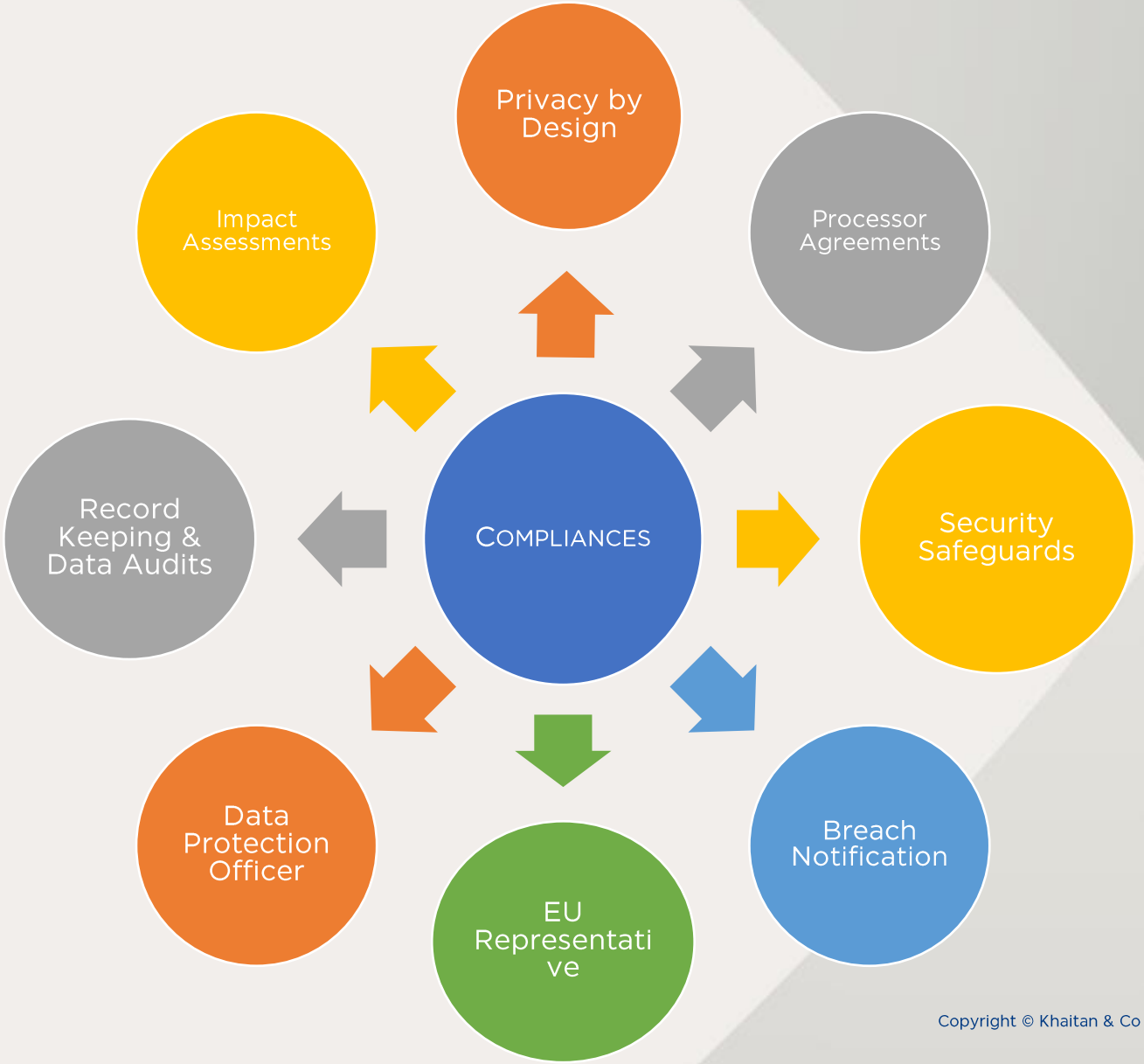
GDPR | Data Subject Rights



GDPR | Key Concepts

- Grounds for processing
  - Consent
  - Necessary for performance of contract
  - Compliance with legal obligation
  - To protect vital interests of Data Subjects or another natural person
  - Public interest and legitimate interest
- Consent in true sense
  - Controller has the onus to demonstrate consent obtained for processing
  - Intelligible and easily accessible form, using clear and plain language
  - Direct nexus to the purpose for which the data is collected
  - Right to withdraw consent / opt-out at any time
  - Child's consent – specific requirements
- Special category 'sensitive' data cannot be processed, except in certain cases (e.g. with consent, in public interest, etc)

GDPR | Key Compliances



GDPR | Cross-border data transfers

- GDPR places restrictions on personal data transfer
- Cross-border data transfers possible to third countries or international organisations subject to GDPR compliance i.e. adequate level of protection
- Data transfer possible in below cases:
  - Within EU member states
  - Countries recognized by the European Commission as providing adequate protection
  - Organization can use BCR – Binding corporate rules (within same corporate group entities)
  - Organization can use EU Model contracts or model clauses with adequate safeguards

Case Law | KS Puttaswamy v UOI

- On 24 August 2017, in a ruling of the Supreme Court in the case of Justice KS Puttaswamy v Union of India, the right to privacy was declared to be a fundamental right under the Constitution of India by a 9:0 majority
- On 26 September 2018, in a separate ruling of the Supreme Court under the same case, the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 ("**Act**") was upheld by a 4:1 majority
- Despite upholding the constitutionality of the Act, several provisions of the have been struck/read down based on certain grounds including infringement of the right to privacy

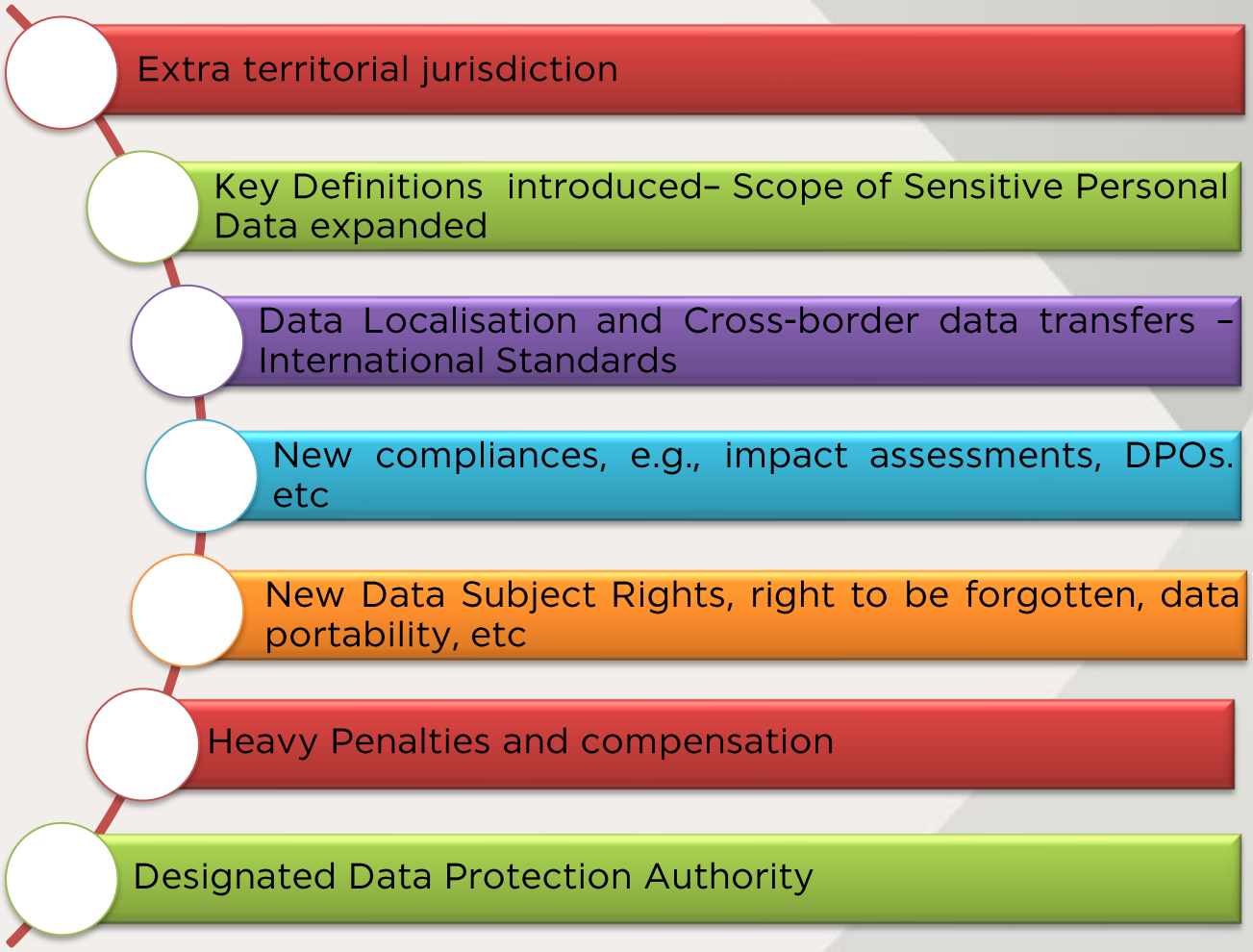
Case Law | KS Puttaswamy v UOI

- Certain key findings of the ruling were:
  - Section 47 of the Act which provided that no Court shall take cognizance of offence under the Act except on a complaint made by the UIDAI should be modified to provide for any individual to be able to make such complaint
  - The mandatory linking of Aadhaar number with bank accounts fails the test of proportionality since the deactivation of the account upon the failure of such linkage would result in depriving a person of her property and would also violate the right to privacy of person with respect to the access to banking details
  - The mandatory linking of Aadhaar number to SIM Cards is unconstitutional in view of the Circular dated 23 March 2017 lacking any authority of law and Section 57 being declared unconstitutional

Case Law | KS Puttaswamy v UOI

- A major impact of the ruling is due to the partial unconstitutionality of section 57 of the Aadhaar Act which enabled body corporates and persons to use Aadhaar
- Section 57 states, "Nothing contained in this Act shall prevent the use of Aadhaar number for establishing the identity of an individual for any purpose, whether by the State or any body corporate or person, pursuant to any law, for the time being in force, or any contract to this effect"
- Post the judgment there is some ambiguity on the reading of section 57 which now may be read as "Nothing contained in this Act shall prevent the use of Aadhaar number for establishing the identity of an individual ~~for any purpose,~~ [~~whether~~] by the State [~~or any body corporate or person~~], pursuant to any law, for the time being in force~~, or any contract to this effect~~"

Personal Data Protection Bill 2018 (Draft Bill) | Overview



Draft Bill | Key Definitions

Data Fiduciary

- Any person, including the State, a company, any juristic entity or any individual who determines the purpose and means of processing of Personal Data

Data Processor

- Any person, including the State, a company, any juristic entity or any individual who processes Personal Data on behalf of a Data Fiduciary but does not include an employee of the Data Fiduciary

Data Principal

- A natural person to whom the Personal Data relates

Personal Data

- Data about or relating to a natural person in relation to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information

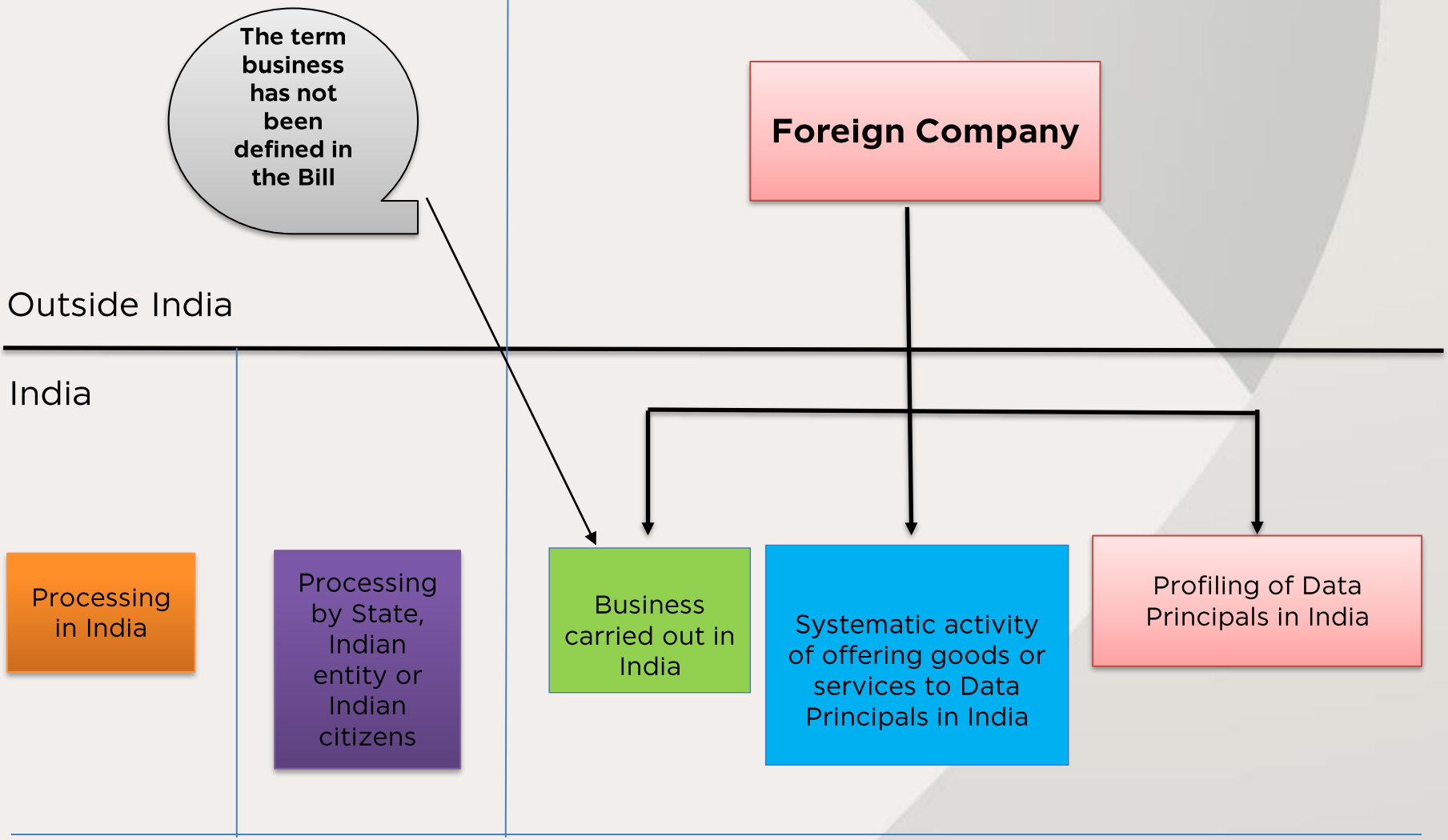
Sensitive Personal Data

- Passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious political belief or affiliation, or any other category as may be specified by the Data Protection Authority of India

Draft Bill | Wider definition of Sensitive Personal Data

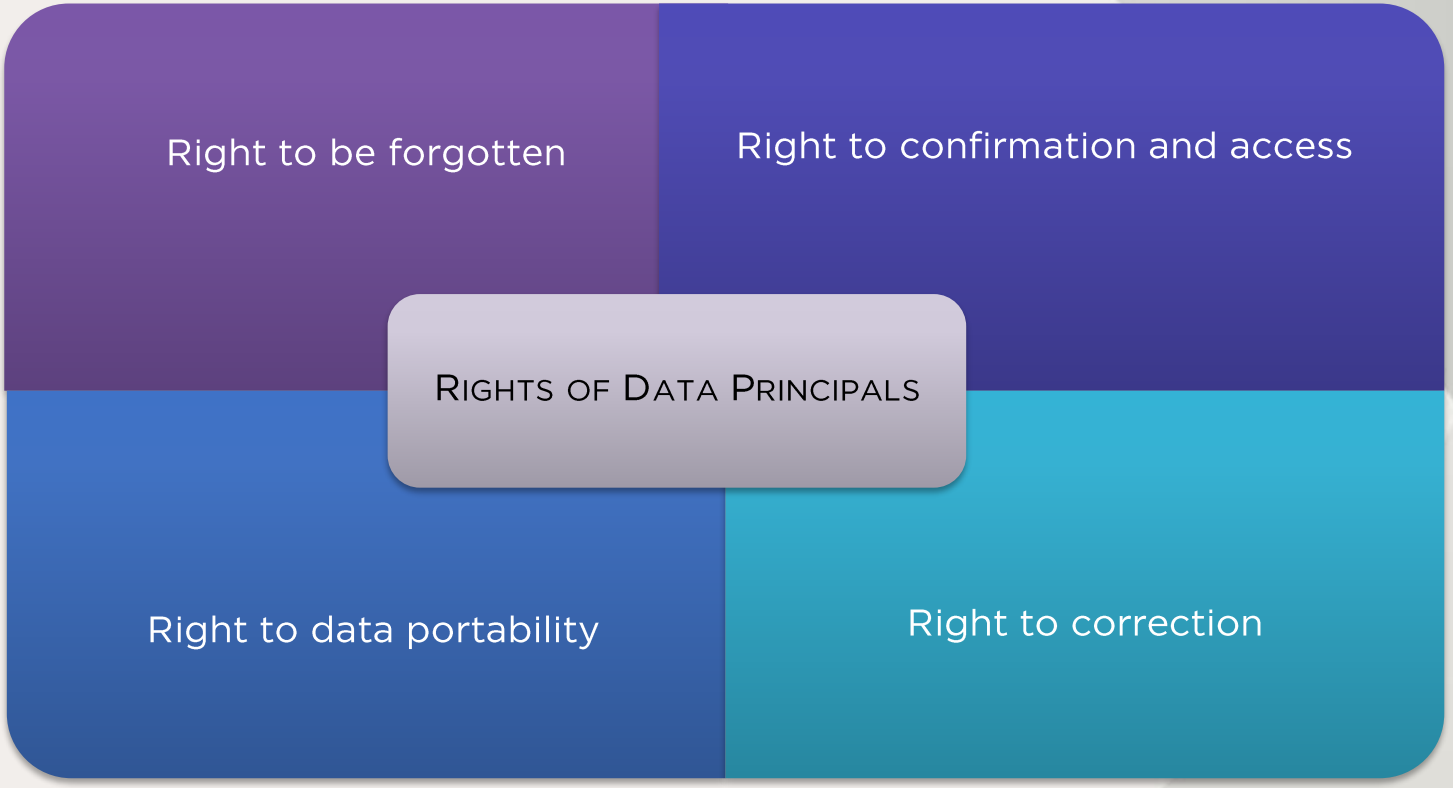
SPDI Rules	Draft Bill
- Passwords - Financial information such as bank account or credit card or debit card or other payment instrument details - Physical, physiological and mental health condition - Sexual orientation - Medical records and history - Biometric information	- Passwords - Financial data - Health data - Official identifier - Sex life - Sexual orientation - Biometric data - Genetic data - Transgender status - Intersex status - Caste or tribe - Religious or political belief or affiliation - Any other category of data specified by the Authority under section 22

Draft Bill | Applicability



Draft Bill | Grounds for Processing of Personal Data

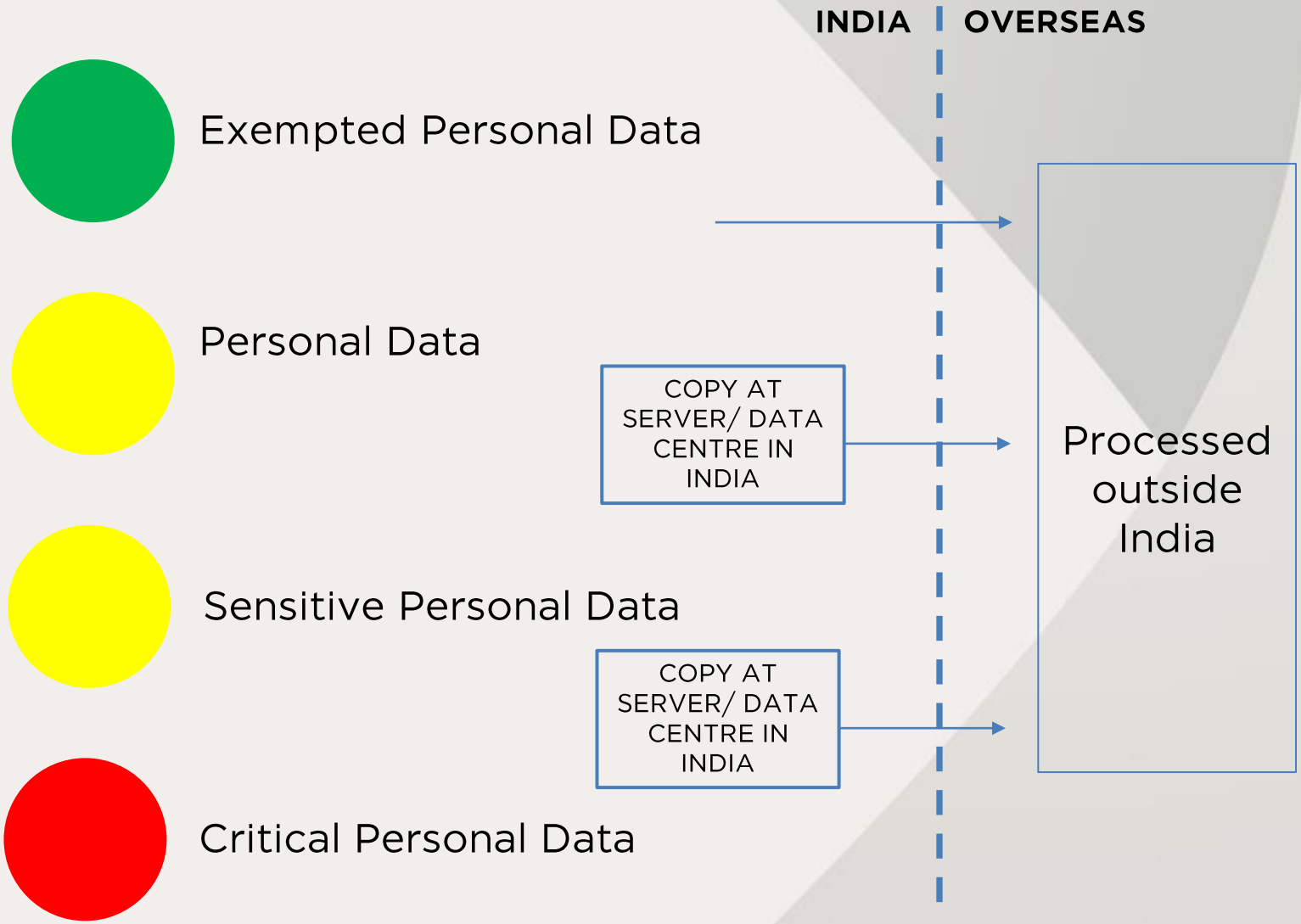
Draft Bill | Data Principal Rights



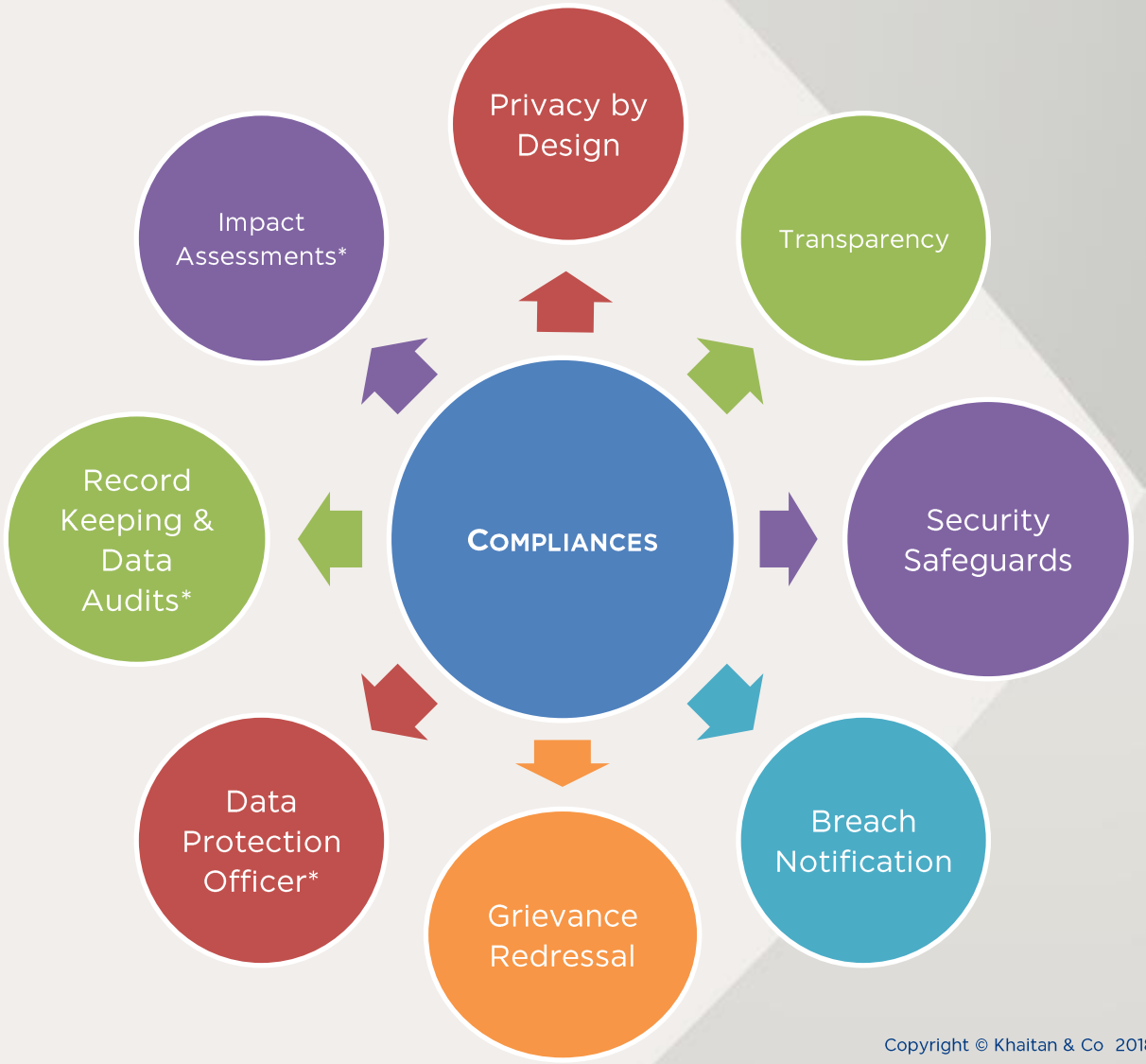
Draft Bill | Cross-border Data Transfer

	Personal Data	Sensitive Personal Data
CONDITIONS	(a) DPA approved Standard Contractual Clauses / Intra-Group Schemes	
	OR	
	(b) Prescription by Central Government after consultation with DPA	
	OR	
	Consent of Data Principal + (a) or (b)	Explicit Consent of Data Principal + (a) or (b)
	OR	
	DPA approves transfer due to situation of necessity	

Draft Bill | Restriction on Cross-border Data Transfer



Draft Bill | Key Compliances - Check the Boxes!



* Applicable to Significant Data Fiduciaries ('SDF')

Draft Bill | Offences and Penalties

- Contravention of provisions related to sensitive personal data, personal data pertaining to children, cross border transfer of personal data etc., INR 150,000,000 or 4% of its total worldwide turnover of the preceding financial year, whichever is higher
- Non compliance with obligations such as conducting a data protection impact assessment, appointment of a data protection officer etc., INR 50,000,000 or 2% of its total worldwide turnover of the preceding financial year, whichever is higher
- Imprisonment for certain offences such as obtaining, transferring or selling personal data in contravention of the Draft Bill

Offences are non-bailable and cognisable

Compensation for harm caused to data principal as determined by the Data Protection Authority

Comparison between EU GDPR and the Draft Bill

PROVISION	EU GDPR	DRAFT BILL
Localisation of personal data	✗	✓
Performance of contract as a ground for processing personal data	✓	✗
Child's consent*	✓	✓
Exemptions*	✓	✓
Data protection officer*	✓	✓
Privacy by design	✓	✓
Rights of data subjects*	✓	✓
Breach notification*	✓	✓
Cross border transfer of personal data*	✓	✓

Comparison between EU GDPR and the Draft Bill (continued)

Provisions	EU GDPR	Draft Bill
Child's consent	• Age of consent is 16 years • May be lowered upto 13 years by member EU countries	• Age of consent is 18 years
Right to be forgotten	• Right extends to erasure of personal data	• Right does not extend to erasure of personal data, but only restricts continuing disclosure of personal data
Breach Notification	• Mandatorily required to notify individuals	• Not mandatorily required to notify individuals • Data Protection Authority of India has the power to determine whether breach should be reported to individuals

Select Best Practices

Follow the 5 P's of Privacy

1. **P**rovider's agreement
2. **P**rivacy policy
3. **P**rocedures for information security
4. **P**ro-active monitoring
5. **P**urge the unnecessary

Best Practice – How Should Consent Be Obtained

Clear and plain language	• Explicit purpose of processing • Scope and consequences • List of user rights • Affirmative actions: silence, pre-ticked boxes and inactivity are inadequate • Separated from others
Withdrawing consent	• Ability to withdraw at any time • As easily as providing consent

Legal Assistance

- Advising on proactive measures to be adopted to address data security
- Advising on dealing with the response to data security breaches
- Training and sensitization of employees
- Drafting of internal and external privacy policies
- Assisting and advising on data protection issues in corporate transactions
- Drafting and negotiating data protection clauses in commercial contracts
- Advising on full range of data protection issues vis-à-vis employees, including monitoring of employees devices, e-mails etc
- General data protection advice

Case Study | Cartelization

- India Co's German parent company received cartelization allegation through its electronic whistleblowing mechanism
- Employees of the India Co were allegedly involved in a cartel and their office equipment were sought to be scanned without their consent

Case Study | Cartelization

- Employer's Code of Conduct / Email / Internet Usage policies could be reviewed
- Mechanism to be devised to review the data within India Co, ring fence SPDI, copy and transfer relevant information to Germany

THANK YOU

www.khaitanco.com