

# Navigating Data Protection and Cybersecurity Challenges for Life Science Companies

---

Eric Carlson, Partner  
Covington & Burling LLP  
September 2017

**COVINGTON**

BEIJING BRUSSELS DUBAI JOHANNESBURG LONDON LOS ANGELES NEW YORK  
SAN FRANCISCO SEOUL SHANGHAI SILICON VALLEY WASHINGTON

[www.cov.com](http://www.cov.com)

# Cybersecurity Law: Key Enforceable Features (I)

---

- Finally taking effect on June 1, 2017, the Cybersecurity Law (“the Law”) is poised to establish uniform regulatory requirements on data protection and cybersecurity, and is currently enforceable in the following ways:
  - Imposing baseline data protection and cybersecurity obligations for “network operators.”
  - Establishing a cybersecurity review mechanism for network products and services that may affect China’s national security.
  - Requiring pre-sale certification of “Critical Network Equipment and Network Security Products.”
  - Stipulating a wide array of sanctions for non-compliant companies.

## Cybersecurity Law: Key Enforceable Features (II)

---

- **Baseline data protection and cybersecurity obligations are applicable to life science companies.**
  
- **Key data protection obligations include:**
  - **Provide notice and obtain consent when collecting or using personal information of Chinese citizens; do not collect personal information if it is not necessary for the services provided (Art. 41)**
  - **Do not disclose, tamper with, or damage citizens' personal information that have been collected; do not provide citizens' personal information to others without consent unless the information is sufficiently anonymized (Art. 42)**
  - **Delete unlawfully collected personal information and amend incorrect information (Art. 43)**

# Cybersecurity Law: Key Enforceable Features (III)

---

- **Key cybersecurity obligations include:**
  - **Implement data security programs according to national standards, effectively respond to network security incidents, prevent illegal and criminal cyber activities, and maintain the integrity, confidentiality and availability of network data (Art. 10)**
  - **Safeguard networks against disruption, damage or unauthorized access, and prevent data leakage, theft, or tampering, including (Art. 21):**
    - Establishing internal cybersecurity management program and protocols, and strictly following access control policies (to limit the access to authorized users and authorized activities);
    - Utilizing the technical measures required to defend against cybersecurity threats such as computer viruses, network attacks, and network intrusion;
    - Utilizing the technical measures required to monitor network security status, log security incidents, and store the relevant network logs for at least six months; and
    - Utilizing data encryption and classification measures as necessary.
  - **Formulate incident response plans and react to security risks in a timely manner; adopt remedial measures and notify users and authorities in case of breach (Art. 25)**
  - **Provide technical support and assistance to authorities in matters relating to national security or criminal investigations (Art. 28)**

# Cybersecurity Law: Implementation Regulations

---

- In order to provide legally binding specifics that detail how aspects of the Law will be applied, various regulators (including the State Council Legislative Office, the Cyberspace Administration of China, the Ministry of Public Security and various sector regulators) are in the process of issuing implementing regulations.
  - To date, this is the only regulation to have been finalized:
    - *Measures on the Security Review of Network Products and Services (Trial)*
  - The following regulations are currently awaiting finalization:
    - *Regulations on the Protection of Critical Information Infrastructure*
    - *Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data (“Cross-border Measures”)*
    - *Several sectorial-specific regulations*
- *Cross-border Measures* likely will be the most relevant implementing regulation for life science companies operating in China.

# Cybersecurity Law: (Draft) National Standards

---

- In addition to implementation regulations, the Chinese government has released drafts of national standards that, while not legally binding, may serve as reference points for enforcers of the Law, most notably:
  - *Information Security Technology – Personal Information Security Specification (the draft “Personal Information Standard”)*
  - *Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (the draft “Cross-border Guidelines”)*
  - *Information Security Technology – Cybersecurity Multilevel Protection Basic Requirements (the draft “Multilevel Protection Requirements”)* and its family of draft standards related to the Multilevel Protection Scheme
- *Personal Information Standard* and *Cross-border Guidelines* offer important guidance to companies on the protection of personal information and on the security assessment of cross-border data transfers.

# Overview of Cross-border Guidelines

---

- On August 31, 2017, an updated draft of the *Cross-border Guidelines* was released for public comments. The comment period ends on October 13, 2017.
  
- Key changes to the previous draft:
  - Definition of cross-border data transfer introduced;
  - Circumstances where a network operators has to conduct a self-assessment and report the result of such self assessment to regulators clarified;
  - Triggers and process of regulator security assessment clarified;
  - Substantive criteria for the security assessment remains largely the same:
    - whether the transfers are lawful, legitimate, and necessary; and
    - evaluating risks associated with the transfers.

# Criminal Law Enforcement

---

- Supreme People's Court and Supreme People's Procuratorate issued an interpretation of criminal law regarding infringement of citizens' personal information in May 2017.
  - Illegal provision of personal information
    - Provision of personal information to a specific person or company or disclosure of such information online or via other means.
    - Even if personal information is lawfully collected, if data subject does not consent to the provision, such illegal provision may lead to serious criminal penalties for both the company and the responsible individual(s).
    - Exclude de-identified data (i.e. identification of a natural person is not possible).
  - Obtaining personal information unlawfully
    - Obtaining citizens' personal information by purchasing, accepting, exchanging, or collecting the information during the process of performing one's duties or providing services.
    - Collecting personal information without consent is viewed as a crime.
      - Case study: illegally obtaining personal information by Nestle's employees from several hospitals by offering kickbacks to healthcare personnel



# Existing Sectoral Rules Governing Healthcare Data (I)

---

- (Electronic) Medical records
  - Various regulations governing medical records, such as *Medical Institution Medical Records Administrative Rules* (2013) (医疗机构病历管理规定) ( 2013年版 )
  - Regulations focus on restriction of access to patient medical records.
    - Access to patient records limited to healthcare professional providing medical treatment to patient, personnel in charge of medical records at medical institution and personnel from relevant health authorities.
    - Other disclosure of patient data prohibited except for treatment, education or research purposes.
  - Obligation rests with medical institutions and healthcare professional.
  - Other types of patient data not covered.

# Existing Sectoral Rules Governing Healthcare Data (II)

---

- “Population health information”
  - National Health and Family Planning Commission (“NHFPC”) issued *Administrative Measures for Population Health Information (Trial Implementation)* (人口健康信息管理办法 (试行)) in May 2014
  - “Population health information” defined broadly to encompass demographic information, electronic health files, electronic medical records, and population health statistics.
  - “Population health information” is expected to be stored in China by “responsible entities” (presumably covering all kinds of medical, health care and family planning services agencies)
    - Data should not be stored in servers located outside of China, even if such servers are owned or rented by “responsible entities.”
    - Requirement potentially extends to third party vendors that provide storage or other information technology services to “responsible entities.”
    - Vague on whether other entities that are receiving “population health information” from “responsible entities” are required store data in China.

# Existing Sectoral Rules Governing Healthcare Data (II)

---

- Genetic data (clinical trial)
  - Data associated with human biospecimens containing the genetic information of Chinese individuals are subject to cross-border transfer restrictions.
  - International collaboration (i.e. clinical trials) must be approved by the Ministry of Science and Technology (MOST) prior to beginning the clinical trial or research study.
    - Specific criteria must be satisfied for cross-border transfer of human genetic resources, including (among others) obtaining informed consent from the “provider” of the human genetic resources and having a “clear” and “reasonable” plan for sharing the information.
    - Regulators now focus on whether the actual physical samples of human genetic resources such as organs, tissues, cells, and bloods are transferred outside of China.
    - Transfer of data associated with the human genetic resources does not need to be approved separately.

# China: The Road Ahead

---

- **Enforcement of data protection and cybersecurity rules**
  - Medical institutions such as hospitals will likely be required to step up their data protection and cybersecurity efforts.
    - Hospitals with massive patient data may be considered as operators of Critical Information Infrastructure (“CII”).
    - *Personal Information Standard* sets the rules for the collection, usage, processing and sharing/transferring of personal information.
      - Healthcare data likely to be considered as “sensitive personal information.”
      - Uncertainties remain for sharing (and receiving) such data through contractual arrangements.
    - Pharmaceutical and medical device companies are unlikely to be considered CII operators, but may be subject to pass on obligations.
  
- **Enforcement of cross-border transfer rules**
  - Population health information is considered “important data.”
  - Cross-border transfers of such data may trigger self-assessment and regulator assessment.
  - Potential sector-specific regulations adding compliance challenges.

# Japan

---

- **Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended (“APPI”))**
- **September 2015: first-ever significant amendment to the APPI (the Amendment)**
- **Personal Information Protection Committee was established on January 1, 2016.**
- **Cabinet Order and the ordinance issued by the Committee (the “Committee Ordinance”) that provide for the details of the Amended APPI were promulgated on October 5, 2016.**
- **The Amended APPI took effect on May 30, 2017**
- **Member of APEC Cross-Border Privacy Rules (established 2011)**

# Korea

---

- **Personal Information Protection Act (“PIPA”) as the overarching law accompanied by various industry-specific laws**
- **Member of APEC Cross-Border Privacy Rules (established 2011)**

# Singapore

---

- **Personal Data Protection Act 2012 (PDPA), plus sector-specific regulations:**
  - **Private Hospitals and Medical Clinics Act (Chapter 248) (PHMC Act), which contains provisions relating to the protection of confidential information such as patients' medical records or treatment or diagnosis.**
  - **Advisory Guidelines for the Healthcare Sector issued by the Personal Data Protection Commission**
- **PDPA requirements on protection of patient data**
- **Retention periods for clinical trial data**

# India

---

- Information Technology Act 2000 (IT Act)
- Sensitive personal data or information (SPDI)
- Data localization?
- August 2017 Supreme Court ruling on constitutional right to privacy



---

# Questions?

Eric Carlson  
[ecarlson@cov.com](mailto:ecarlson@cov.com)  
Covington & Burling LLP (Shanghai)



***THE EVOLVING WORLD  
OF PRIVACY***

---

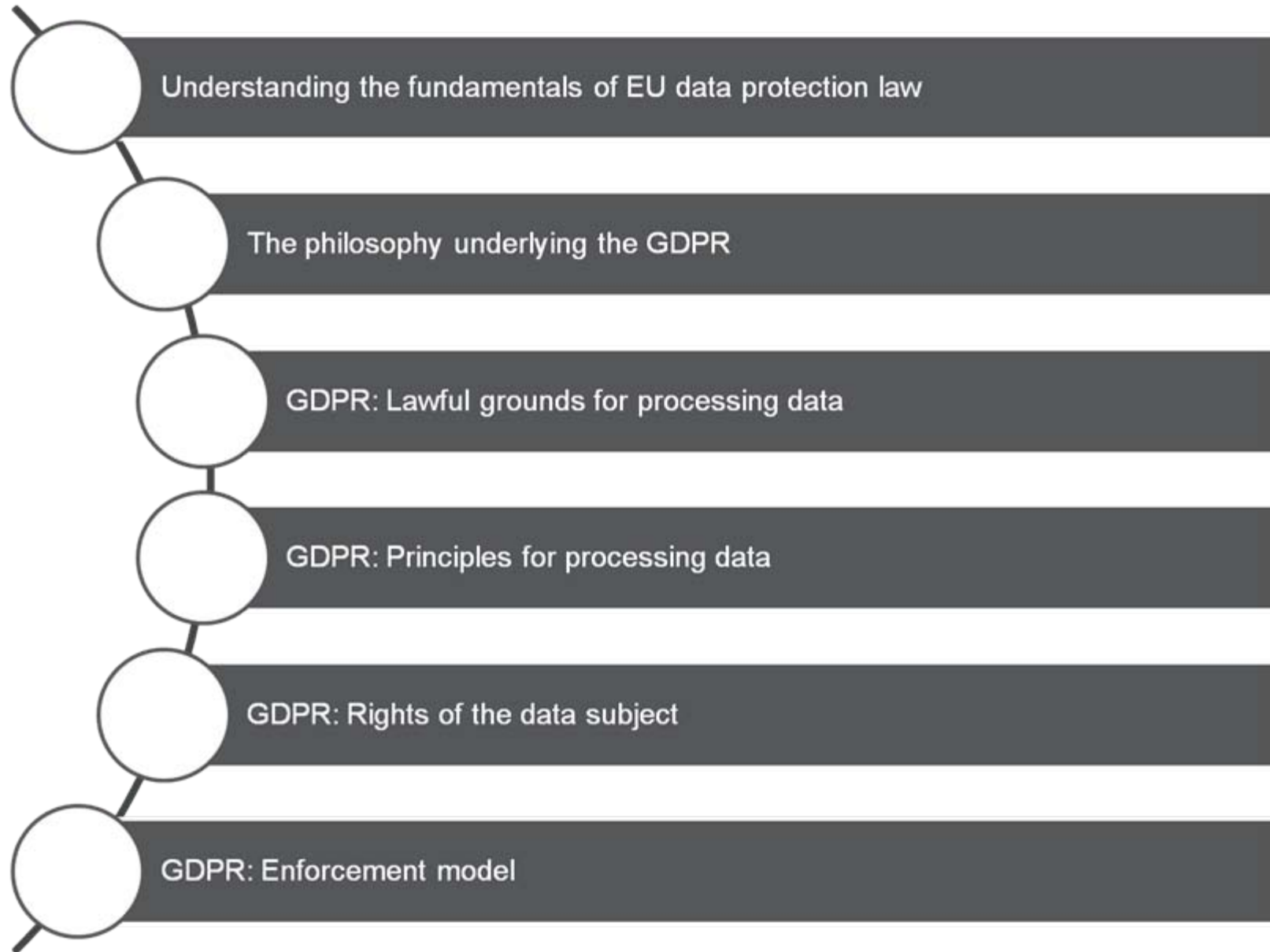
BUILD. MANAGE. PROTECT.

NAVIGANT

# TOPICS COVERED TODAY

- **Overview of GDPR – What Does This Mean**
- **Why Privacy Matters in the EU**
- **Fundamentals of GDPR**
- **Overview of Critical Elements**

# GENERAL DATA PROTECTION REGULATION - OVERVIEW



# UNDERSTANDING THE FUNDAMENTALS OF EU DATA PROTECTION LAW

europari.europa.eu

## *Article 7*

### **Respect for private and family life**

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

## *Article 8*

### **Protection of personal data**

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.

## “RULES OF THE ROAD”/ “OPACITY SHIELD”

### **CJEU:**

“legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter” (*Schrems*, §94; 2015)

### **German Constitutional Court:**

“[the personality right] includes the authority of the individual to decide for himself, on the basis of the idea of self-determination, when and within what limits facts about his personal life shall be disclosed. The individual’s decisional authority needs special protection in view of the present and prospective conditions of automatic data processing” (*BVerfGe* 65, 1; 1983 – translation by Kommers)

# EARLY DATA PROTECTION LAWS IN THE EU



# WHY ALL THE FUSS?

## Comprehensive Application of Rules

- Material
- Personal
- Territorial scope

## Significant Increase in Fines

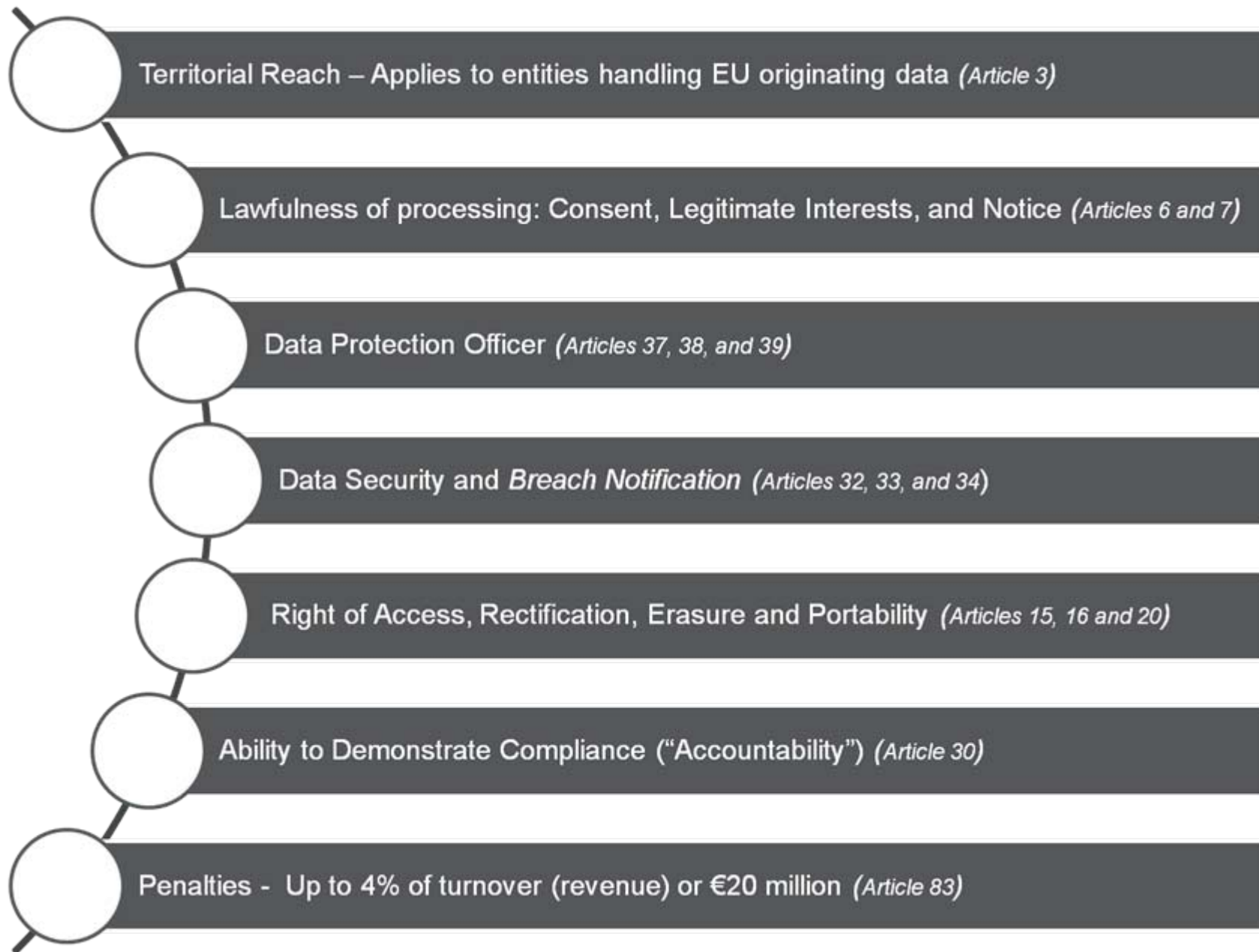
- 20M EUR or 4% of global annual turnover
- **Largest fines under current rules:**
  - ICO: 400.000 pounds, 2016, Talk Talk for a data breach
  - CNIL: 150.000 EUR to Google in 2014, right to be forgotten

## New Substantive Rules:

- Accountability, right to data portability, class actions
- **Comprehensive Material Scope:**
  - Personal Data: Any information related to an identified or identifiable individual (art. 4(1))
  - Processing of Personal Data: Any operation or set of operations which is performed on personal data or on sets of personal data (art. 4(2))



# GDPR – CRITICAL ELEMENTS



# SCOPE AND EXCEPTIONS

## Exceptions

- processing takes place outside the scope of EU law (e.g. national security of a MS); law enforcement; by a natural person in the course of a purely personal or household activity

## Wide territorial scope

- ... in the context of the activities of an establishment of a controller or a processor in the EU, **regardless of whether the processing takes place in the EU or not**
- ... processing of data of data subjects by controllers/processor **who are not established in the EU**, if they **offer goods or services to data subjects in the Union or if they monitor their behavior.**

## Comprehensive personal scope

- “data subject” = all natural persons within the EU, irrespective of legal status (citizens, residents, refugees; Art. 8 Charter – “everyone”)
- “controller” = alone or jointly with others, determines the purposes and means of the processing of personal data (art. 4(7))

# IDEAS UNDERLYING THE GDPR

## Recital 4

- The processing of personal data should be designed to serve mankind.

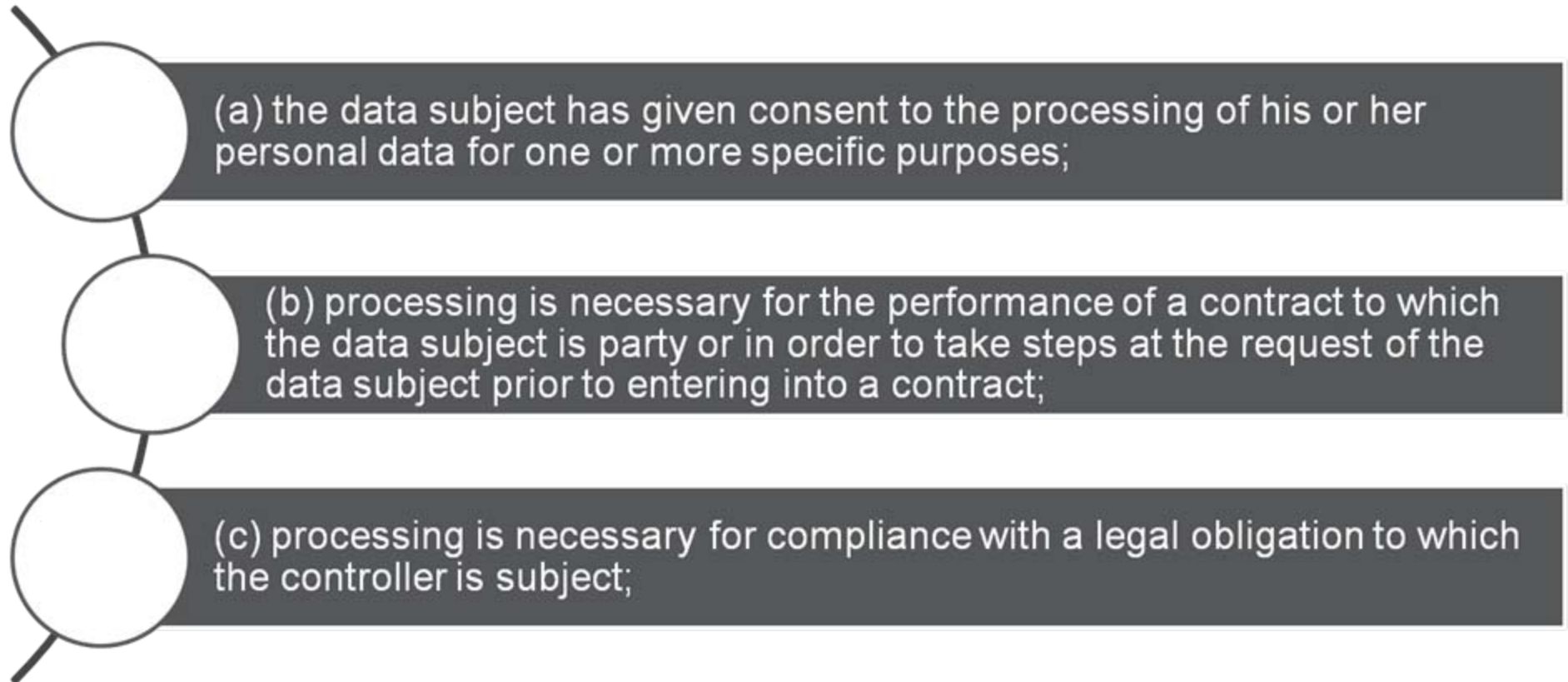
## Recital 7

- Natural persons should have control of their own personal data.

## Recital 10

- Ensuring a “consistent and high level of protection of natural persons” and removing “obstacles to flows of personal data”

# ARTICLE 6(1): LAWFUL GROUNDS FOR PROCESSING DATA (1 OF 2)

- 
- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
  - (b) 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;
  - (c) processing is necessary for compliance with a legal obligation to which the controller is subject;

# ARTICLE 6(1): LAWFUL GROUNDS FOR PROCESSING DATA (2 OF 2)



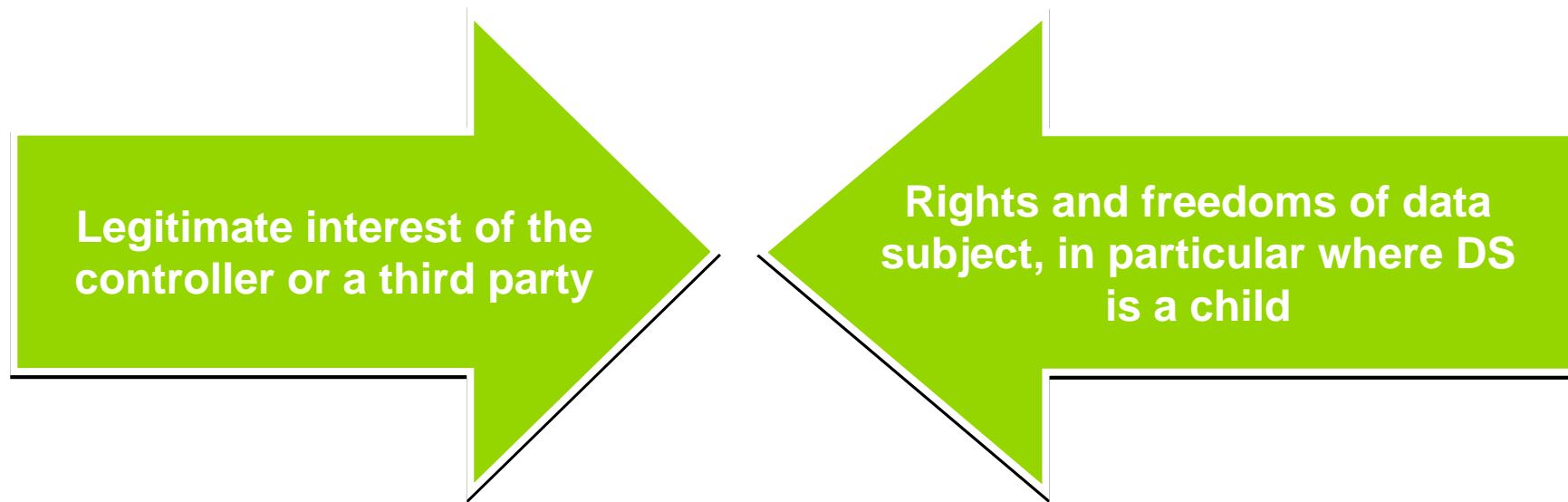
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) 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;

(f) 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.

# LEGITIMATE INTEREST OF THE CONTROLLER

Processing of data on the legal ground of legitimate interest always requires a balancing exercise:



**Guidance:** Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (April 9, 2014)

- (a) assessing the controller's legitimate interest,
- (b) impact on the data subjects,
- (c) provisional balance and
- (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects.

# IDEAS UNDERLYING THE GDPR

## Quality of Consent – Art. 4(11)

- Freely given
- Specific
- Informed
- Unambiguous

## How?

- Statement
- Clear Affirmative Action

### Compliance

- Controller must be able to demonstrate compliance

### Consent

- If given together with terms of service, consent form must be “distinguishable”, “intelligible”, “easily accessible”

### Withdraw Consent

- Using clear and plain language
- Data subject has the right to withdraw consent at any time

### Freely Given

- The provision of a service conditional on consent to the processing of personal data that is not necessary for the performance of that service?

# GDPR: RIGHTS OF THE DATA SUBJECT

**Right to information – art. 13, art. 14**

**Right to access – art. 15**

**Right to rectification – art. 16**

**Right to erasure - art. 17**

**Right to restriction of processing – art. 18**

**Right to data portability – art. 20**

**Right to object – art. 21**

**Right not to be subject to a decision based on profiling  
– art. 22**



# RESPOND TO REQUESTS AND COMPLAINTS FROM THE DATA SUBJECTS

## Key Requirements

### 1. Rights of the data subjects

- Right to access personal data (Article 15)
- Right to accuracy, update or correct data (Article 16 and 19)
- Right to opt out of processing (Articles 7, 18 and 21)
- Right to data portability (Article 20)
- Right to be forgotten / erasure (Articles 17 and 19)

## Practical Solutions

**Intake** - Enhance your support desk inquiry intake system to identify if the inbound request is related to a GDPR centric obligation and ensure the resulting ticket is routed the correct team member.

**Repeatability** - Provide the team member fielding the request a series of checklists and templates which she can use to respond to the data subject. These tools will drive repeatability and standardization when responding to the data subjects, such as communication protocols, encryption process and standard formats.

### Right of Erasure

- Using the data inventory developed in a prior requirement, identify the data repositories containing PI sourced to EU data subjects.
- Prepare a checklist and workflow diagram outlining the steps required to purge or mask a data subject's data from your environment.
- Review data retention policies for backup tapes or other data storage repositories.

# MAINTAIN DOCUMENTATION TO DEMONSTRATE COMPLIANCE AND/OR ACCOUNTABILITY

## Key Requirements

1. GDPR Article 24 - Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall:
  - implement appropriate technical and organizational measures to ensure and to
  - **be able to demonstrate that processing is performed in accordance with this Regulation.**
  - Those measures shall be reviewed and updated where necessary.
2. Accountability principle
  - Article 30 – Data Inventory

## Practical Solutions

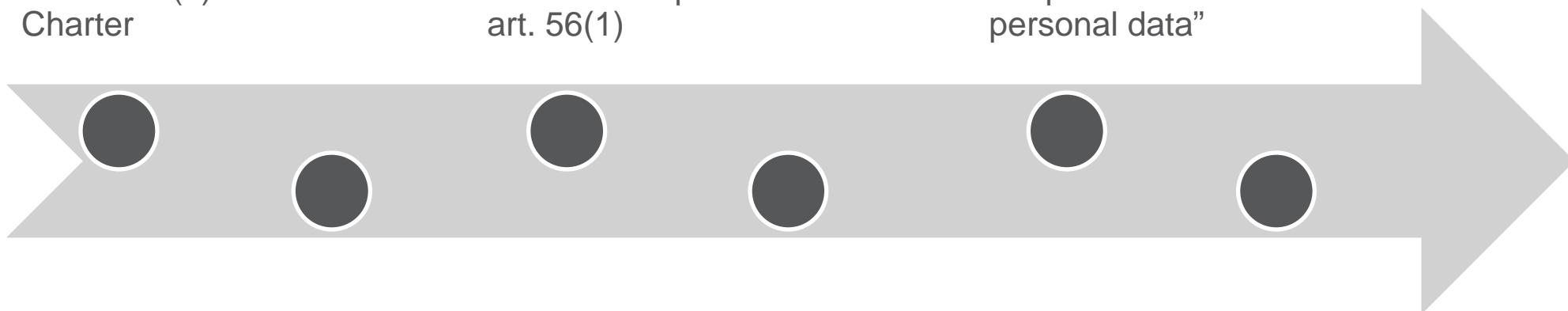
1. GDPR report in the form of a playbook.
  - Executive summary includes the steps undergone to be able to demonstrate compliance with GDPR.
  - The body of the report encompasses the deliverables created during project fieldwork and other evidence documentation associated with privacy framework.
  - Updated at least annually
2. Third party project management tracking platforms

# GDPR: ENFORCEMENT MODEL

Independent supervisory authorities (Data Protection Authorities - DPAs) – Article 8(3) Charter

Lead supervisory authority - the supervisory authority of the main establishment or of the single establishment of the controller or processor – art. 56(1)

Tasks of DPAs – art. 57 (a) to (v): “fulfil any other tasks related to the protection of personal data”



Each EU Member State has one DPA (Germany has 1 federal and 16 state-level)

HOWEVER, each DPA is competent to handle a complaint lodged with it if the subject matter relates only to an establishment in its Member State (absence of cross-border element) or substantially affects data subjects only in its Member State.

Powers of DPAs – art. 58:

- Investigative
- Corrective
- Authorization and advisory powers
- Powers to engage in legal proceedings
- All powers are subject to effective judicial remedies and due process

## FURTHER READING

- Handbook on European data protection law issued by the Fundamental Rights Agency of the EU
- [Article 29 Working Party Opinions and Recommendations](#)

THANK YOU!

J. Mark Farrar

[mark.farrar@navigant.com](mailto:mark.farrar@navigant.com)

+1 404 575 3800