

# Introduction to GDPR

Helene Millenaar

Global Risk and Compliance Director

Centrient Pharmaceuticals

# AGENDA

What is GDPR?

GDPR grants rights to data subjects

Responsibilities of companies under GDPR

What if your company does not comply with GDPR?

Status of data protection in India



# Speaker Bio

- Helene Millenaar is Global Risk and Compliance Director with Centrient Pharmaceuticals. She is responsible for all compliance related topics at Centrient Pharmaceuticals, which include anti-bribery, corruption, export control, privacy and competition law.
- Before that she was global head of investigations and director competition law at Nouryon (formerly AkzoNobel Specialty Chemicals) where she conducted internal investigations on a wide variety of compliance-related topics. She also advised Nouryon and before the split, the AkzoNobel businesses on the full range of competition law issues that include behavioral issues, merger control, and competition law compliance. Prior to joining AkzoNobel, Millenaar was a senior associate at the Dutch law firm Stibbe in Amsterdam and at Clifford Chance in Amsterdam and Brussels, advising clients on EU and Dutch competition law.
- In 2017 Helene finalized a two years' executive master of compliance and integrity management at the VU in Amsterdam (NL). She studied at the Universities of Leiden (NL), Barcelona (SP) and London (UK).



# What is GDPR?

- GDPR is the European Union's General Data Protection Regulation (GDPR)
- It is the toughest privacy and security law in the world
- GDPR was put into effect on May 25, 2018
- If an organization processes personal data of EU citizens or residents, or if it offers goods or services to such people, then **the GDPR applies even if the organization is not in the EU**
- Fines for violating the GDPR are very high



## Some important terms...

- **Personal data** — Personal data is any information that relates to an individual who can be directly or indirectly identified

Examples of personal data: names and email addresses but also location information, ethnicity, gender, health, biometric data, religious beliefs, web cookies, and political opinions

- **Data processing** — Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing... so basically anything
- **Data subject** — The person whose data is processed. These are your customers or site visitors
- **Data controller** — The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you
- **Data processor** — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations

# GDPR grants rights to data subjects

The GDPR grants several new rights for the data subjects, being

- Control over when, how, and why companies can collect and use a subject's personal data
- Access to the personal data that companies and organizations collect from him or her

Right to be informed

Right of access

Right of rectification

Right to erasure

Right to restrict processing

Right to data portability

Right to object

Right in relation to automated decision making and profiling

# Responsibilities of companies under GDPR

The GDPR restricts how, why, and when companies can use the personal data of data subjects

According to the GDPR a company is responsible for the personal data that it uses. This means that:

▪ Companies will need to assess whether the processing of personal data is allowed



▪ Companies must know how to conduct privacy maintenance



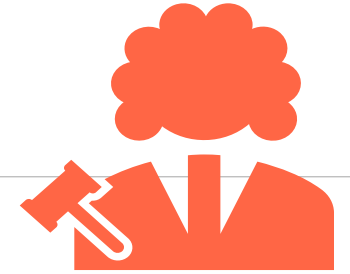
▪ Companies must embed privacy within their organization



▪ Companies must communicate about privacy



# Is the processing of personal data allowed?



## It is important to consider:

- Lawfulness of processing personal data
- Principles applicable to processing of personal data (being (i) lawfulness, fairness and transparency, (ii) purpose limitation, (iii) data minimization, (iv) accuracy, (v) storage limitation, (vi) integrity and confidentiality and (vii) accountability)
- Demonstrable consent of data subject (if consent is used as the legitimate ground for the processing)
- Transfer of personal data outside the EU
- Special categories of personal data (such as ethnicity, political opinions, religious beliefs, health, sexual orientation)
- Additional protection for children under 16



# How to conduct privacy maintenance?



It is important to consider:

- Implementation and documentation
- Data Processing Agreements (DPA)
- Risk analysis and Data Protection Impact Assessments (DPIA)
- Policies and implementation of technical and organizational measures to protect personal data
- Systems and processes to ensure data subject's rights, such as data portability
- Retention

# How to embed privacy within your company?



## It is important to consider:

- Data Protection Officer
- Rights of data subjects (access, correction, deletion, objection)
- Data breach notification
- Trained staff
- Data protection by design / default: relevance of privacy for (developing) products and services
- Certification
- Supervision

# How to communicate about privacy within your company?



## It is important to consider:


- Clear and comprehensible communication, e.g. Privacy Statement
- Data breach notification procedure
- Contact details of DPO
- Objection to profiling
- Openness about records of processing activities
- Communication with the Supervisory Authority

# What if your company does not comply?

Not complying with the GDPR is a risk for everyone

If an EU Supervisory Authority traces a breach back to your company organization, it can have severe consequences, such as:






- Your company could face steep fines
- Impact on your company's reputation
- Increased risk of scams and financial damage to the people whose data was exposed

+ British Airways – €204,600,000 

+ Marriott International – €110 390 200 

## TOP 5 BIGGEST GDPR FINES

\*Only includes final & binding fines

	Google Inc.	€50,000,000
	TIM - Telecom Provider	€27,802,946
	Austrian Post	€18,000,000
	Deutsche Wohnen SE	€14,500,000
	1&1 Telecom GmbH	€9,550,000

# Status of data protection in India



- Information Technology Act of 2000
- Personal Data Protection (PDP) Bill was introduced in Parliament in 2019 which incorporates many elements of GDPR, such as:
  - Requirements of notice and prior consent for the use of personal data
  - Limitation on purposes for which data can be processed
  - Data minimization
  - Compliance requirements for data processors
  - Appointment of DPOs within companies
  - Right to data portability
  - Regulation and supervision by a proposed Data Protection Authority
- There are two main differences between PDP Bill and GDPR, being:
  - Provision of criminal penalties for harm arising from violations of PDP Bill
  - Relationship between a data processor and its consumer is a fiduciary relationship
- Revised draft of the PDP Bill is expected to be issued in 2021

# Status of data protection enforcement in India



## Enforcement

- No national regulatory authority for protection of personal data
- PDP Bill proposes a Data Protection Authority

## Fines

- IT Act: fines of up to INR 500,000 when there is disclosure of personal information in breach of a lawful contract or without consent
- PDP Bill: penalties linked to worldwide turnover. Those penalties can range from 2% or 4% of the worldwide turnover, depending on the type of breach

## Criminal liability

- IT Act: imprisonment of up to three years when there is disclosure of personal information in breach of a lawful contract or without consent
- PDP Bill: imprisonment of three years for re-identifying personal data or sensitive personal data without the consent of the concerned individual

# Case law on data protection in India



## Supreme Court Privacy Judgment

There have been a number of judgments in the courts on privacy matters but there is no significant court regulatory practice on the application of these provisions

## Some useful links:

- GDPR (including useful recitals): <https://gdpr-info.eu/>
- FAQ about GDPR: <https://gdpr.eu/faq/>
- Checklist for organizations to achieve GDPR compliance: <https://gdpr.eu/checklist/>
- UK Information Commission's Office (handy tools): <https://ico.org.uk/>
- Resources on IAPP which is global information privacy community: <https://iapp.org/resources/>
- Overview of data protection in India: <https://www.linklaters.com/en/insights/data-protected/data-protected---india>





# CONTACT



[pscinitiative.org](http://pscinitiative.org)



[info@pscinitiative.org](mailto:info@pscinitiative.org)



Annabel Buchan:  
+55 (11) 94486 6315



[PSCI](#)



[@PSCInitiative](#)

WeChat

[制药供应链组织PSCI](#)

For more information about the PSCI please contact:

#### PSCI Secretariat

Carnstone Partners Ltd  
Durham House  
Durham House Street  
London  
WC2N 6HG

[info@pscinitiative.org](mailto:info@pscinitiative.org)

+55 (11) 94486 6315

#### About the Secretariat

Carnstone Partners Ltd is an independent management consultancy, specialising in corporate responsibility and sustainability, with a long track record in running industry groups.

**carnstone**  
partners ltd