

SmartKarrot GDPR Training April **2020**



Table of Contents

Overview **GDPR**

- 01 General Overview of GDPR
- 02 What constitutes “Personal Data”? and The Life Cycle of Personal Data
- 03 Basis of data processing (lawful)?
- 04 Types of personal data

Processing **Principles**

- 05 The Life Cycle of Personal Data
- 06 Basis of data lawful processing
- 07 Principles relating to processing of personal data

Rights & **Penalties**

- 08 Rights of the data subject
- 09 Roles for a GDPR Organization
- 10 Penalties

What, why & how?

General Data Protection Regulation

What is **GDPR compliance**?

- New set of rules designed to give EU citizens more control over their **personal data**.
- It deals with **Personally Identifiable Information (PII)** of natural citizens within the EU.

Why **GDPR compliance**?

- Data **breaches**.
- Data **lost**.
- **Enforces legal obligation** that maintains records of personal data.

How **did it come**?

- **25th April 2015**: Data Protection Act scrapped.
- **27th April 2016**: European Parliament passed a regulation act “2016/679” which came to be known as GDPR.
- **15th May 2016**: Entire EU and member states enacted GDPR for its citizens.
- **31st April 2017**: Every organization that operates in EU/ collects information about EU citizens are expected to be GDPR compliant.

Want to **know more?**

[Art. 5-11 GDPR](#)



What constitutes **Personal Data?**

Any data or a pseudonymized data can still fall under the definition of **personal data** if that data allows a living person to be directly, or indirectly identified from it.

Personal data is so important under GDPR because individuals, organizations, and companies are made accountable to the data they hold or process.

What constitutes **Personal Data?**

- 01 Fitness & activity data
- 02 Opening bank account
- 03 Smartphone app usage & GPS data
- 04 Personality traits
- 05 Interest & Preferences

- 06 Actively record responses for a survey
- 07 Observe on social media
- 08 Emotions & desires
- 09 Values and beliefs



Feel



Say



Think



Do



Identified:
Cindy Roberts

What constitutes **Personal Data for SmartKarrot?**



01 Cookies (SK Landing Page)

02 Emails for Newsletters

03 Sales demo data

04 User Attributes (Username, Email, Gender, Phone...)

05 Device Attributes (Device ID, IP Address)

06 Log Events (An example of pseudonymized data)

07 Users of SK Platform (CSM, Admin, Executive...)

08 Employee data of SmartKarrot Organization

Types of

Personal Data

Want to **know more?**

[Art. 5-11 GDPR](#)



PII Identifier

- 01 Your Name
- 02 Identification Numbers
- 03 Location Data
- 04 Online Identifier

PII Sensitive

- 01 Genetic Data
- 02 Biometric data, including facial recognition and fingerprint records.
- 03 Health Data
- 04 Racial or Ethnic origin
- 05 Religious or philosophical beliefs
- 06 Trade union memberships
- 07 Sex life or sexual orientation

The Lifecycle of **Personal Data**



Want to **know more?**

[Art. 5-11 GDPR](#)



Basis of Data **lawful** **processing**

Want to **know more?**

[Art. 5-11 GDPR](#)



Legal



Contractual



Legitimate Interest



Consent



Vital Interest



Public Interest

lawful processing

Processing is
lawful only if

**at least one
of this
applies**



Legal Obligations

The controller is obliged to process personal data for **legal** obligations.



Consent

The **consent** of data subjects to the processing of his/her personal data



Contractual Necessity

Processing is needed in order to enter or perform a **contract**.



Vital Interest

It is **vital** that specific data are processed for the matters of life and death.



Legitimate Interest

There is a weighted & **legitimate** interest where processing is needed, and the interest is not overridden by others.



Public Interest

Public authorities and organizations in the scope of public duties and interests.

Principles relating to **processing of personal data**



Legal



Fairness



Transparency



Purpose



Minimization



Accuracy



Storage Limit



Integrity



Accountability

Want to **know more?**

[Art. 5-11 GDPR](#)



Principles relating to **processing of personal data**

SmartKarrt



Lawfulness

If no **lawful** basis applies, then the **processing** is unlawful and in breach of this **principle**. **Lawfulness** also means that controllers and processors cannot do anything with the personal **data** which is unlawful in a more general sense



Fairness

In general, **fairness** means that **processing** must be done in ways that people would reasonably expect and not in ways that have unjustified adverse effects on them. Assessing whether **processing** is **fair** depends in part on how the **data** was obtained and how the **processing** affects individuals.



Transparency

The principle of **transparency** requires that any information and communication relating to the **processing** of those personal **data** be easily accessible and easy to understand, and that clear and plain language be used.



Purpose

The principle of **transparency** requires that any information and communication relating to the **processing** of those personal **data** be easily accessible and easy to understand, and that clear and plain language be used.

Principles relating to
**processing of
personal
data**

SmartKarrt



Minimization

Procure & Process personal data **limited** to what is **necessary** for the purpose for which they are processed (not excessive). Focus on storage limit.



Accuracy

Personal data shall be **accurate** and, where **necessary**, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or **rectified** without delay.



Storage Limit

So, even if you collect and use personal **data** fairly and lawfully, you cannot keep it for longer than you actually need it. This is up to you, and will depend on how long you need the data for your specified purposes (**Exempt 8(1)**)



Integrity

Integrity and **confidentiality** to process personal data in a manner that ensures appropriate security, protection against **unauthorized** or **unlawful processing** and **accidental loss, destruction** and **damage**.



Accountability

The **accountability** principle requires controllers and processors to take responsibility for their processing activities and for how they comply with data protection **principles**.

Rights of the **Data subject**

Every data subjects have the following 6 **rights**



Transparency



Rectification &
erasure



Restrictions



Information & access
to personal data



Right to object and
automated individual
decision - making



Notified on breach

Want to **know more?**

[Art. 12-23 GDPR](#)



Rights of the **Data subject**



Transparency

Transparency implies that any information and communication concerning the processing of personal data must be easily accessible and easy to understand.



Information & access to personal data

The provision of **right of access** means that controllers/DPO are required to provide **data subjects**, i.e., natural persons whose personal information is being collected, a copy of their processed personal data upon request



Rectification and Erasure

Data subject have the right to have personal data concerning him or her rectified and a '**right to be forgotten**' where the retention of such data infringes this Regulation or Union or Member State law to which the controller/DPO is subject.



Right to object and automated individual decision - making

The **data subject** shall have the right not to be subject to a decision based solely on **automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.



Restrictions

The provision of **right of access** means that controllers/DPO are required to provide data subjects, i.e., natural persons whose personal information is being collected, a copy of their processed personal data upon request



Notified on breach

EU data protection law gives data subjects the **right to restrict** the processing of personal data about them in certain circumstances. This means that a data subject can limit how an organization uses data about him/her. This is an alternative to requesting data erasure.

Roles for a **GDPR Organization**

Want to **know more?**

[Art. 24 - 43 GDPR](#)

These are the must have **roles for a GDPR compliant organization**. But for most SaaS (B2B types) companies, they have **data processor** and **data protection officer** at their end while the controller is the business entity with which they have signed the contract.



Controller



Data Processor



Data Protection Officer

Roles for a **GDPR** Organization



Controller

The **data controller** determines the purposes for which and the means by which personal **data** is **processed**. So, if your company/organization decides 'why' and 'how' the **personal data** should be **processed** it is the **data controller**.



Data Processor

Design, create, and implement IT **processes** and systems that would enable the **data controller** to gather personal **data**. Use tools and strategies to gather personal **data**. Implement security measures that would safeguard personal data. Store personal data gathered/sent by the data controller.



Data Protection Officer

The **data protection officer** is a **mandatory role** for all companies that collect or process EU citizens' personal data. DPOs are responsible for educating the company and its employees about compliance, **training** the staff involved in data processing, and conducting regular **security** audits.

Administrative fines

If the fault is on **Controller, Data processor or the Data protection officer**



Administrative fines up to **10,000,000 EUR**, or in the case of an undertaking, up to **2% of the total worldwide annual turnover of the preceding financial year**, whichever is higher.

If the fault is on **basic principles for processing, consent, data subject rights, audit failure or noncompliance, no notice of data breach.**



Administrative fines up to **20,000,000 EUR**, or in the case of an undertaking, up to **4% of the total worldwide annual turnover of the preceding financial year**, whichever is higher.

In Conclusion

First GDPR Compliant Company

- **QXRS** Becomes the First GDPR Compliant Company in India, 26th June 2018.
- **Exponea** becomes the first GDPR-certified SaaS company in the world, 25th May 2018.

Total SaaS Companies

- Since GDPR is **self certification** so there is no official record of how many companies worldwide are GDPR certified.
- But from gathered information, it ranges from **1.5 L to 2.3 L SaaS companies worldwide.**

SaaS companies fined so far

- **Google**, 2019-01-21, €50 million
- **Bisnode** (business, credit and market information), 2019-03-15, €220,000
- **Marriott** International

GDPR fines & notices

To see **complete list**,
[click here](#)



Company/Organization	Amount	Reason
Google (France)	€ 50 Million	Insufficient transparency, control, and consent over the processing of personal data for the purposes of behavioral advertising
Marriott international (UK)	£ 99 Million	Failure to undertake sufficient due diligence when acquiring Starwood hotels group, whose systems were compromised in 2014, exposing approximately 339 million guest records .
British Airways (UK)	£ 183 Million	Use of poor security arrangements that resulted in a 2018 web skimming attack affecting 500,000 consumers .
Cathay Pacific (Turkey)	£ 88,000	Failure to implement necessary technical and administrative measures to ensure data security and breaching notification obligations

GDPR fines & **notices** (Contd.)

To see **complete list**,
[click here](#)



Company/Organization	Amount	Reason
La Liga (Spain)	€ 250,000	Poorly disclosing purpose for requesting GPS and microphone permissions within the football league's mobile app.
Facebook (US)	\$ 2.2 Billion	For storing millions of passwords insecurely
Facebook (UK)	€ 1.5 Billion	Passing sensitive information to Cambridge Analytica

GDPR fines & **notices** (funny ones)

To see **complete list**,
[click here](#)



Company/Organization	Amount	Reason
Takeaway Restaurant (Austria)	€ 1,500	GDPR-fine for CCTV at a takeaway restaurant that covered the street and a nearby gas station without privacy notice.
Small SME (Germany)	€ 10,000	Fined for not appointing a DPO
A Software SME (Germany)	€ 1,000	For using employees' photographs from Facebook on their employee database and organization page.
Party Organizers (Austria)	€ 800	Awards a natural person the personal data ("party preference") which was processed by the Austrian Postal Corp. without legal basis
A start-up for branding and digital marketing in Ireland (Ireland)	€ 2,000	For forcefully storing cookie information of users without allowing them to give a no for the consent

About **SmartKarrot**

SmartKarrot helps drive business outcomes around life-time value, retention, expansion, adoption, engagement and customer experience. One integration engine connecting behavioral analysis, strong personalized engagement and automated actions.

For more details contact:

info@smartkarrot.com



Thank You