

**Springer Nature  
GDPR**

**Gerald Coppin**

**Deputy Group Data Protection Officer**

**15 March 2018**

**SPRINGER NATURE**

# Introduction

- The new **General Data Protection Regulation (GDPR)** will take effect on **25 May 2018**
- GDPR applies to any data we hold that can be linked to an identifiable person, whether that be customers, authors, students, teachers, staff or job applicants
- It impacts how the data is gathered, stored, processed, transferred, and deleted, and sets out certain security standards. This means it impacts our processes and systems.
- It also mandates the documentation of processes and systems
- If we fail to comply with the new legislation, we could see revenue loss, reputational damage and incur fines of around 60 million euros

# Overview of Springer Nature's approach

- The **GDPR project team** has been working for the past year to set up a compliance program that will enable the Springer Nature group to become and remain compliant with the GDPR in a scalable and efficient manner
- We've created a **new Data Protection Office**
- We conducted an **initial gap analysis** which helped us to identify our priority areas of focus
- We've introduced a **new global data protection framework** including a new **Data Protection and IT Security Policy, data protection guidelines, the Springer Nature privacy compliance portal** and **templates** to help us comply with the GDPR, which will be implemented as a global standard and which will all be available to all staff via internal intranet

## Overview of Springer Nature's approach (cont'd)

- In order for new processes and systems to be set up in a compliant way, we will provide **training** on the new framework on to all staff, with more tailored training via our online learning and development platform to follow for those teams that handle personal data

# 1. > The GDPR: Introduction

## ■ What is “Personal data”?

- Any information relating to a living individual who can be identified from that data or from that data in addition with other information in your possession.
  - Examples: a person’s name, address, e-mail address, phone number, employee number (direct identifiers) or any information linked with such identifiers (e.g. age, salary).

## ■ What is “Processing”?

- The term is interpreted very broadly and encompasses any use of personal data.
- Processing begins when the data is first obtained and only ends after its deletion or destruction.

# 1. > The GDPR: Introduction

## ▪ **General rules for data processing**

When using personal data you have to:

- Only collect data for the purposes specified (in order to process personal data for another purpose than the initial one, numerous requirements have to be fulfilled),
- Minimize the amount of data to what is necessary in order to achieve the desired purpose,
- Keep data accurate and up to date,
- Do not store data longer than necessary to achieve the purpose for which the data was collected, and
- Ensure the data's integrity and confidentiality.

## 2.1.1 > Introduction

- **The GDPR imposes various requirements for processing of personal data**
  
- Organizational requirements, e.g.
  - Documentation requirements
  - Maintaining a Record of Processing Activities
  - Conducting Data Protection Impact Assessments (“DPIA”)
  - Maintaining a system for Data Breach Notifications
  - Implementing technical and organizational security measures for processing of data
  
- Material Requirements
  - Data processing is forbidden unless specifically permitted by consent/law
  - Special legal requirements exist for outsourcing data processing and transferring data to countries outside the EU

## 2.1.2 > Material Requirements

- **Under the GDPR, personal data only can be processed lawfully if there is either**
  - valid **consent of the person concerned**, or
  - some other form of **legal justification**;  
**otherwise, any use of personal data is forbidden.**



## 2.1.2.1 > Consent

- **Requirements for data subject consent are very high**
- Consent must be
  - Freely given: The individual must have a real choice whether he declares consent
  - Specific and informed: Consent must be clear and concise, covering the details of the data use (e.g. what data is used, for how long, who has access, how can the consent be revoked...)
  - Unambiguous: Consent must generally be “opt-in”, not be implicit

## 2.1.2.3 > Processing Activities Involving Third Parties

- **Transferring data from one Springer Nature entity to another**
- No privileges or exemptions apply to the transfer of personal data within the Springer Nature Group.
- Every data transfer to another Springer Nature entity or a third company is unlawful unless covered by consent or another legal justification.

## 2.1.2.3 > Processing Activities Involving Third Parties

### ▪ **Involvement of Data Processors**

- In case a Springer Nature entity acts as a processor, it has to fulfil additional requirements under the GDPR.
- Springer Nature has created a guideline “Springer Nature as a Data Processor” accessible to all staff

## 2.1.3 > Organizational Requirements

### ▪ **Technical and Organizational Security Measures**

- The GDPR requires companies to implement technical and organizational measures to ensure the data processing is secure
  - Examples: Encryption, Pseudonymization, Access Limitation, Back-up Systems, Password protection
  - Data protection starts at your desk. Please
    - Activate screen locks whenever you leave the office,
    - Use passwords that have at least 12 characters,
    - Do not store passwords in public spaces, e.g. on your desk, and
    - Do not leave documents lying around where they might be seen by unauthorized personnel.

## 2.2 > Data Subject Rights

- **Under the GDPR, data subjects have multiple rights to ensure transparent and fair processing. (1)**
  - Those rights include:
    - The right to be informed about the data processing: Data subjects must be informed in detail, pro-actively and in a transparent manner about the intended data processing, including the purposes of the intended processing, any envisaged (cross border) data transfer and the respective retention periods.
    - The right of access: Data subjects can request access to their personal data held by the respective Springer Nature entity.
    - The right to rectification: Data subjects have the right to have incomplete or incorrect personal data rectified.

## 2.2 > Data Subject Rights

- **Under the GDPR, data subjects have multiple rights to ensure transparent and fair processing. (2)**
  - Those rights include:
    - The right to erasure: Data subjects can, under certain circumstances, require the respective Springer Nature entity to delete their personal data.
    - The right to restriction of processing
    - The right to data portability
    - The right to object to processing

## 3 > Take Home Essentials

- **Data protection starts with data collection but does not end there**
- **No processing of personal data is permissible without justification**
- **Always secure and minimize the processing of data**
- **Acknowledge the rights of data subjects**
- **Document all data protection efforts**

Questions

**SPRINGER NATURE**