WILLIAM FRY

// PRIVACY SOURCE

# GDPR and Employment

The General Data Protection Regulation (**GDPR**), which took effect on 25 May 2018, is one of the most ground-breaking pieces of EU legislation in the digital era.

It has modernised the legal framework of data protection and privacy in Europe to ensure the consistent protection of personal data by making businesses more accountable for compliance.

**Some key challenges and impacts of the GDPR for employers include:**

## PENALTIES & CLAIMS

Fines as high as €20million or 4% annual global turnover (whichever is greater) may be imposed for breaches of the GDPR. Employees may also take legal action against employers for material and non-material damage (e.g. stress, humiliation) suffered due to an employer's failure to process their personal data as required by the GDPR.

## NEW & ENHANCED RIGHTS FOR EMPLOYEES

Enhanced rights include the right to erasure, right to restriction of processing, right to object to processing, right of access and right to data portability. Employers need to ensure that requests from employees exercising these rights are processed without undue delay (and in any event within one month) and free of charge.

## EMPLOYEE DATA PROTECTION NOTICES & POLICIES

More detailed data protection notices and updated policies are required. Employers' data protection notices and policies need to be more prescriptive and transparent regarding the processing of personal data. Any notice or policy drafted pre-GDPR will likely need to be replaced or updated.

## PAYROLL & OTHER SERVICE PROVIDERS

Service providers (eg payroll) must be vetted to confirm their ability to comply with the GDPR. A contract containing obligations prescribed by the GDPR also needs to be entered into between employers and service providers. Service providers must flow down their obligations to any sub-contractors processing personal data relating to the employees of such an employer.

## RECORDS OF PROCESSING ACTIVITIES

Most employers are required to keep and maintain detailed records of all processing activities under their responsibility. Each record must be a "living document" and may be examined or inspected by the Data Protection Commission should it conduct an audit or investigation.

## MANDATORY SECURITY BREACH REPORTING

Security breaches related to employee personal data must be reported to the Data Protection Commission within 72 hours where there is a risk to the rights and freedoms of employees. Employees must be notified about the breach without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

## MANDATORY DPO (DATA PROTECTION OFFICER)

A DPO must be appointed where an employer's core activities consist of regular and systematic monitoring on a large scale or large processing of special categories of personal data (eg health data) or if any employer is a public authority or body.

## FOREIGN DIRECT INVESTMENT & EXPANDED TERRITORIAL SCOPE

The GDPR expanded the territorial scope of data protection law such that non-EU organisations may come within its scope (eg where they process the personal data of EU-based employees).

## PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

Data protection principles cannot be an afterthought under the GDPR. Building data protection principles into the design and default settings of new technologies, business processes and projects is mandatory for employers.

## DPIAS (DATA PROTECTION IMPACT ASSESSMENTS)

Employers are required to conduct a DPIA where new technologies, business processes or projects involve high risk processing of employee personal data such as profiling and large-scale processing of special categories of data such as data concerning physical or mental health (or health status), biometric data, trade union membership, etc.

# GDPR & Employment

## ACCOUNTABILITY | NEW & ENHANCED RIGHTS | ENFORCEMENT

# Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partners below, our your usual William Fry contact.

**David Cullen**
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

**Leo Moore**
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

**John O'Connor**
PARTNER
+353 1 639 5183
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA