Simmons & Simmons

GDPR and HR
The Headlines

February 2018

GDPR Overview

- Harder to obtain consent
- More fair processing information has to be provided to the individual
- Obligation to keep comprehensive records of processing activities
- Increased requirements for contracts with data processors
- New rights for individuals e.g. 'right to be forgotten'
- Notification requirements in the event of a data breach

Consent and notification:

The GDPR makes the ground of consent an uncertain legal basis for processing personal data. In particular, consent is likely to be unworkable in an employee data context. Consent as a legal ground for processing should be avoided - other grounds should be relied upon wherever possible

- Consent – personal data
  - ICO guidance suggests consent is agreement or clear, affirmative action
  - Consent must be freely given, specific, informed and unambiguous
  - Imbalance of power in employment relationship – consent will not be 'freely given' so cannot be legal basis for processing
  - Consent can be withdrawn at any time
- Consent – sensitive personal data
  - If sought, consent must be explicit
  - ICO guidance suggests that clear, affirmative action unlikely to suffice for explicit consent

Under the GDPR, data subjects are entitled to receive fair processing information from data controllers processing their personal data. Many employers are choosing to provide a data privacy notice setting out this information. In order to prepare a notice, HR needs to have a clear understanding of the extent and nature of data processing activities

- Notification – fair processing information includes
  - Data controller identity
  - Purpose for processing personal data and legal basis
  - Recipients of personal data
  - Detail of international transfers of personal data
  - Outline of data subject rights

Data retention

- Personal data should not be retained for longer than necessary for the purpose for which it was originally collected/processed
  - GDPR not prescriptive
  - However, good opportunity to assess what personal data HR stores and for how long (e.g. through a data retention policy)
  - Keep in mind that minimisation of personal data processing is key for compliance with the GDPR. Avoid keeping employee documentation 'just in case'

Data Subject Access Requests

As yet, ICO have not published GDPR-specific DSAR guidance - previous guidance still helpful on the concept of proportionality.

- Data subject right to
  - A copy of the personal data
  - Information relating to purpose of processing, categories of personal data processed, recipients of personal data, retention periods and others
- Timing
  - Response without undue delay and within one month
  - Extension of further two months possible if requests are complex / numerous
- Fee
  - Information must be provided free of charge (no longer able to request a fee)
  - If request is manifestly unfounded or excessive, a fee may be charged in respect of administrative costs of providing information (i.e. should not be arbitrary fee)
- "Manifestly unfounded" / "excessive" requests
  - Controller can charge reasonable fee or refuse to act

To do:

Speak to your organisation

- is there an organisation-wide process taking place?
- can you seek input and knowledge-sharing from other divisions?

Audit and scoping exercise

- assess and establish what personal data you process
- map your data-flows (for example, intra-group, to third parties)
- establish what personal data you store and where, and for how long
- establish what security measures are in place (for example, who can access some categories of personal data)

Triage approach

- the amount of change can be overwhelming
- take a risk-based approach by looking at the risk of the personal data processing activity against the level of corrective action required to comply with the GDPR and allocate a Red/Amber/Green status
- work through items on your RAG action list methodically

Update documentation, policies and systems

- using the information you have gathered in your scoping exercise, make informed changes
- concept of data privacy 'by design' in your department
  - you can create an environment where data privacy is in-built
  - by having template employee documentation, creating/updating policies to be used day to day, organising training and increasing awareness of data protection principles, you can ensure the 'way of doing things' is GDPR-compliant

Philip Bartlett
Partner
T +44 20 7825 4470
E philip.bartlett@simmons-simmons.com

Elizabeth Wake
Managing Associate
T +44 20 7825 4265
E elizabeth.wake@simmons-simmons.com

Beth Hammond
Associate
T +44 20 7825 5759
E beth.hammond@simmons-simmons.com