The General Data Protection Regulation

Sophie White and David Widdowson, Abbiss Cadres LLP

REBA Innovation Day 2017 – 23 November 2017

ABBISS CADRES
YOU AND YOUR PEOPLE

Law & Tax
People Consulting
Communications

Abbiss Cadres – Who we are

- We are subject matter experts in multiple disciplines touching all aspects of the employment relationship.
- We provide broad People Consulting and Communications expertise alongside regulated legal and tax services.

- Our practice is specially licensed to enable all our disciplines to be represented at partner level. It is a unique and innovative practice model.

ABBISS CADRES
YOU AND YOUR PEOPLE

Law & Tax
People Consulting
Communications

The General Data Protection Regulation (GDPR)

- Data Protection Bill to implement GDPR –second reading in the House of Lords on 10 October 2017
- Organisations must comply by **25 May 2018**
- Employers must consider their obligations in processing employee data. In relation to rewards this includes;
    - Pay
    - Pension Data
    - Insured Benefits Data
    - Gender Pay Gap Data
    - Incentives Data

GDPR: the headlines

- ✓ Familiar concepts and framework: not a total overhaul
- ✓ Use it as an opportunity to engage with staff
- • BUT this requires a change of mindset because this is more than tick boxing – “data protection by design”.

ABBISS CADRES
YOU AND YOUR PEOPLE
Law & Tax
People Consulting
Communications

GDPR: the headlines

- ✕ Wider territorial scope
- ✕ Increased financial penalties
- ✕ More onerous accountability and governance requirements
- ✕ Requirement to report breaches

GDPR changes: territorial scope

- Businesses and employers **within** the EU which process personal data (regardless of where that processing takes place)
- Businesses and employers **outside** the EU which process personal data relating to individuals within the EU in some circumstances.
- Opportunity to allocate primary regulator within the EU
- Still problematic because of loss of safe harbor, but
    - Privacy shield
    - Binding Corporate Rules referenced
    - EU standard clauses

GDPR changes: penalties

- Penalties for breach will increase, up to the greater of 4% of annual worldwide turnover / EUR20M
- Some EU states may impose criminal penalties
- In the UK the bill currently envisages 2 new offences;
  - Intentionally or recklessly re – identifying individuals for anonymised or pseudonymised data, or knowingly handling or processing such data;
  - Altering records with intent to prevent disclosures following a data subject access request.

GDPR changes: Accountability and Governance

- Controllers must positively demonstrate compliance

✓ More than ‘responding to breaches or complaints’
✓ Impact assessments
✓ Audits
✓ Activity records for larger organisations
✓ Appoint a Data Protection Officer for some organisations

- Implement “privacy by design “ in any new processes

GDPR changes: Portability of Data with service providers/Data processors

- Tighter rules on the use of DPs (those who process data on behalf of data controllers, for example, outsourced payroll providers) :
    - extends the formal contractual requirements between data controllers and DPs
    - places new obligations on DPs to
        - ensure data security
        - demonstrate compliance to the controller and
        - permit inspection and audit.
- Update third party contracts to ensure they include mandatory protection

GDPR changes: consent as the basis for data processing

- Common to obtain in UK employment contracts to process data
- BUT not freely given and not valid
- Now needs to **be as easy to withdraw as it was to give**
- If 'use consent' then RIGHT TO BE FORGOTTEN
- Identify other lawful basis for processing – is it necessary to perform the contract of employment or to comply with a legal obligation (gender pay gap reporting, AE)?
- How about sensitive personal data e.g. health records/private medical insurance?
    - Valid explicit consent
    - Necessary for carrying out employment rights and obligations and employer has appropriate policy document in place

GDPR changes: requirement to report breaches

- Breach of security leading to accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data
- Notify to data protection authorities, promptly, usually within 72 hours
- What about a breach by one of your rewards providers?

GDPR: what should businesses be doing now?

- ! Escalate - on the internal radar ASAP
- ! ‘Privacy Champions’ - appoint a senior person/set up a committee to be responsible for GDPR compliance
- ! Assess whether to appoint a Data Protection Officer
- ! Data audit and data cleanse
- ! Review policies and procedures
- ! Review contractual documentation – especially consent for employees and contracts with third parties
- ! Train managers and teams on the new requirements

ABBISS CADRES
YOU AND YOUR PEOPLE

Law & Tax
People Consulting
Communications

Any questions?

Sophie.White@abbisscadres.com

David.Widdowson@abbisscadres.com