Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Pensions

Data protection and pensions

Briefing

January 2016

Trustees of pension schemes should be aware of their data protection obligations. This briefing seeks to remind trustees of the relevant data protection principles, including those relevant to choosing and documenting relationships with administrators, and certain developments affecting schemes which have relied previously on the US safe harbour network.

Application – Data Controller v Data Processor

The Data Protection Act 1998 (DPA) applies to a person who, either alone or jointly, determines the purpose for and manner in which, personal data is processed (known in the DPA as a 'Data Controller'). A Data Controller can be either an individual or an incorporated company and therefore covers both individual and corporate trustees.

In contrast, pension scheme administrators and advisors will in the large majority of cases be classed as 'Data Processors' as they will be processing the personal data on behalf of the trustees. In general, the primary obligations in the DPA fall only on the Data Controllers, although pension scheme trustees cannot absolve themselves of their obligations under the DPA, Data Processors can be held to account by the Data Controller for any breaches of the DPA they cause the Data Controller to commit through contractual clauses imposed by the Data Controller on the Data Processor in the contractual arrangements between the parties.

In cases where the pension scheme administrators and advisors independently, or jointly with the trustee, determine the purposes for which the personal data is to be processed, they may be classed as a joint Data Controller and will have their own primary liability under the DPA in respect of the processing of any personal data for which they are joint controller. Please contact us if you would like further information on whether your pension scheme administrators and advisers are data processors or joint data controllers.

Processing Personal Data and Sensitive Personal Data

Trustees should be aware that the DPA imposes obligations with respect to the 'Processing' of personal data. Processing is broadly defined and includes the adaptation or alteration of the data, using the information or data, storing the information, disclosure of information or otherwise making that information or data available, or the erasure or destruction of information.

Likewise, the definition of 'Personal Data' is wide and includes not only information relating to a living individual who can be identified from that data, or from that data and other information that is, or is likely to come into the possession of, the trustees of a pension scheme, but also any expression of opinion about the individual or indications of the intentions of the pension scheme trustees or any other person in respect of that individual.

Additional obligations apply to the processing of 'Sensitive Personal Data'. The most relevant category of 'Sensitive Personal Data' for pension scheme trustees is information relating to a person's physical or mental health. In the pensions context this would include medical evidence submitted in support of ill health early retirement applications and trustees should ensure the appropriate additional DPA principles are complied with in respect of such information.

Trustees will generally obtain consent to process data as part of the application form the member signed on joining the scheme. However, trustees should review this language to ensure it provides for adequate consent to the processing the trustee is undertaking. In particular, historic language may not be sufficient to cover all of the purposes for which the personal data is being processed and may not extend to consent for processing of sensitive personal data (for which consent must be explicit).

The Eight Principles

The DPA imposes eight principles that must be complied with by trustees (as Data Controllers) when processing personal data. The DPA sets out in detail further considerations and requirements relevant to each principle. For the purposes of this note we consider in more detail principle 7, which is of key consideration to pension scheme trustees, and recent developments to principle 8.

Principle 1

Personal data must be processed fairly and lawfully. Additional requirements need to be satisfied in respect of sensitive personal data for the processing of such data to be considered fair and lawful (see principle 7).

Principle 2

Personal data shall be obtained only for one or more specific and lawful purposes and shall not be processed in any manner incompatible with such purpose or purposes.

Principle 3

The personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.

Principle 4
Personal data shall be accurate, and where necessary, kept up to date.

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or purposes.

Principle 6
Personal data shall be processed in accordance with the rights of the data subject under the DPA. The DPA includes a number of rights which apply to the data subject whose personal data is being processed. This includes the right, in certain circumstances, to be supplied with certain information regarding the processing of personal data, such as the purpose for which data is being processed and the recipient of that data.

Principle 7
Appropriate technical and organisational measures should be taken against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Pension scheme trustees who use external pension scheme administrators to run the pension scheme will remain responsible for ensuring that adequate security measures are taken in respect of the personal data. As a result, trustees should ensure that they comply with certain obligations when:

- choosing an administrator
- documenting the arrangements with the administrator.

When choosing a third party administrator to process personal data, trustees should ensure that the administrator provides sufficient guarantees in respect of the security measures governing the processing of the relevant data and that the security measures the administrator will implement in respect of the personal data are adequately documented. The trustees should ensure that the written contract they have with the administrator contains robust obligations on the administrator in respect of the personal data, including:

- an obligation that the administrator is only to act on instructions from the trustees
- that it is to comply with obligations equivalent to those imposed on the trustees by the seventh principle of the DPA
- and that it is to implement and comply with an agreed security schedule that details the required security measures (this security schedule should be appended to the contract).

Similar considerations are likely to apply in the context of liability management exercises where the trustees may need to share information with employers.

If sensitive personal data is involved, trustees may well also need to obtain express consent from members.

Principle 8

Personal data shall not be transferred outside the European Economic Area unless the country to which it is transferred ensures an adequate level of protection for the rights and freedoms of the individuals who are the subjects of the relevant personal data.

Data Processors operating in the US used to be able to sign up to the safe harbour framework which allowed the companies to self-certify their adherence to a number of 'Safe Harbor Principles' which largely mirrored the EU's own data protection principles. This automatically authorised these companies to accept data transfers from the EU. However, in *Maximillian Schrems v Data Protection Commissioner Case* C-362/14 the CJEU held that the US safe harbour rules no longer met EU standards (the DPA stemming from the principles enshrined in EU law). The ruling could have wide-reaching implications for pension schemes and it could, in particular, impact pension schemes with:

- US members
- US parent companies or US group companies who manage the administration for all group pension arrangements
- third party administrators with servers in the US.

Pension scheme trustees should therefore review their agreements with scheme administrators to see if those agreements rely on the US safe harbour framework. For trustees relying on the US safe harbour framework, a replacement system of adequate protection (currently either EU model clause or binding corporate rules) will need to be considered and put in place promptly as enforcement action is planned to commence from the end of January 2016 against any entities who do not have adequate protection in place.

Please contact us if you require assistance in putting these alternative arrangements in place.

Enforcement

The enforcement provisions in the DPA include the ability of the Information Commissioner to require Data Controllers to comply with the eight principles by issuing an enforcement notice. Failure to comply is a criminal offence and may also result in civil liability if there is damage.

The Information Commissioner can currently issue a fine of up to £500,000 on Data Controllers if:

- there has been a serious contravention of the principles
- the breach is likely to cause substantial damage or distress
- the breach was either deliberate or reckless.

An example – Scottish Borders Council 2012

A data processing company was employed by the Scottish Borders Council (SBC). That company disposed of former employee pension files at a recycling facility at a supermarket. A member of the public noticed these files at an overfilled recycling bin and alerted the police. The information contained names, addresses, dates of birth, National Insurance numbers, salary, bank account details, death benefit nominations and reasons for leaving the pension scheme.

SBC was not aware that the data processing company had been disposing of files in this way (which they had been doing for a number of years). Nevertheless, the Information Commissioner's Office imposed a fine of £250,000 on SBC.

SBC appealed and the First Tier Tribunal (Information Rights) held that the data processing arrangements contravened the DPA and that the contravention was serious. SBC had sent a general email to the data processing company in 2005 asking whether any guarantees or assurances as to security and confidentiality of data could be provided but had taken no further action. Further, no written contract with the processing company nor contractual clause requesting that the processing company only acts on SBC's instructions existed.

Whilst on appeal, the fine was reversed because the tribunal held that there was not a sufficient likelihood of substantial damage or distress, a breach of the DPA had occurred due to SBC's insufficient monitoring and documenting of the obligations of the data processing company.

Changes to the law

The European Union (EU) has been debating how it will reform its data protection regime since January 2012. On 15 December 2015, the Civil Liberties Committee (LIBE) of the European Parliament issued a press release announcing a provisional political agreement between the European Parliament and Council negotiators on the texts of both the General Data Protection Regulation (GDPR) and the Police and Judicial Cooperation Data Protection Directive. Formal approval by the Council and the European Parliament is expected in early 2016, after which the legislation will be published in the Official Journal. These new provisions will apply two years later, likely in the first quarter of 2018.

Key changes that will be introduced by the GDPR include:

- maximum fines that can be imposed for non-compliance will be increased to 4 per cent of worldwide turnover
- export non-compliance will be in the GDPR's maximum fine tier (this is particularly important following the decision in the Schrems case in which it was decided that the US safe harbour framework was invalid)
- privacy notices and consent wordings and mechanisms will need to be reviewed and in most cases amended to meet the new requirements
- data processors will have direct liability under the new regulation to data subjects for damages and regulators will have the ability to fine them for breaches of the data protection responsibilities imposed on them by data controllers.

Conclusion

Trustees should remain aware of their primary obligations under the DPA, including the requirements to monitor and document the obligations of any data processors to whom they transfer personal data. Given the quantum of fines which can be imposed and the impending enforcement action arising from the *Schrems* judgment, trustees should check that their current arrangements remain fit for purpose.

If you would like further advice on the obligations of pension scheme trustees under the DPA, please contact your usual pensions and data protection contact.

Contacts

If you would like further information please contact:

Peter Ford
Partner, London
Tel +44 20 7444 2711
peter.ford@nortonrosefulbright.com

Lesley Browning
Partner, London
Tel +44 20 7444 2448
lesley.browning@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.