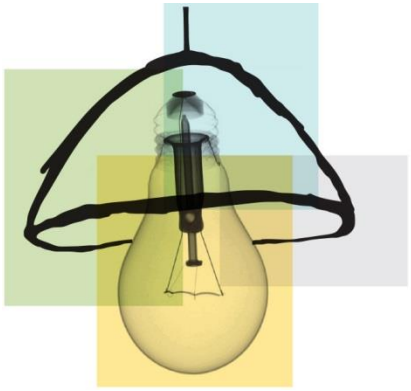

E-rostering and Collaborative Banks

Guidance note on the impact of GDPR

E-rostering

E-rostering is growing in popularity amongst NHS organisations as an alternative to paper based rostering. Where a software programme is purchased and used by an NHS organisation for this process, the organisation will be both the data controller and the data processor in respect of the data which is processed.

Alternatively, an external organisation may be used to process personal data for e-rostering or, as part of the software programme, IT support may be provided by an outsourced software provider (for instance using a 'software as a service' or 'platform as a service') which results in personal data of employees being processed by that provider. In these scenarios, it is essential that there is an agreement in place between the data controller and data processors.

The General Data Protection Regulation (GDPR) sets out that:

"Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller."

As the Information Commissioner's Office (ICO) guidance points out, data controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. This means (1) undertaking due diligence on the proposed provider; and (2) ensuring that there is a written contract in place which meets the requirements of GDPR.

Contracts must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Controllers remain directly liable for compliance with all aspects of the GDPR (including the activities of outsourced processors), and for demonstrating that compliance. If this is not achieved then they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures and it is, therefore, vital that agreements which are put in place with processors deal with liability and contain indemnities.

Collaborative Banks

Integrated care is one of the key elements of the government's approach to improving the health service for patients and collaborative working between NHS organisations in respect of bank work is a key factor in achieving integrated care and efficiencies. NHS Improvement is encouraging Trusts to set up collaborative banks.

Collaborative banks take many forms and so specific advice on the documents which need to be put in place in order to comply with the GDPR will need to be dealt with on a case by case basis. However, where Trusts, as data controllers, will share the personal data of bank workers between each other, a data sharing agreement is recommended to comply with the GDPR principle of transparency.

We look below at aspects which require consideration in the context of collaborative banks.

DBS Checks

CQC guidance states that where people take up a new position and who are currently working in services regulated by CQC. i.e. at another Trust, that individual can satisfy the expectation that they will have an appropriate DBS check if they can provide evidence of a check, at the right level for their role, that is less than three months old at the point of application.

The guidance goes on to state that people supplied by an employment agency can satisfy the expectation that they will have an appropriate DBS check if they can provide evidence of a check that is less than 12 months old. Our view is that a collaborative bank is unlikely to be an employment agency and so the standard three month rule will apply.

Use of the DBS Update Service allows an applicant to apply for a DBS check only once and then, if they subsequently need a further check of the same type, to use their existing certificate and an employer can review whether any changes have occurred. This would appear to be the most efficient way of carrying out DBS checks for staff who are part of a collaborative bank.

Right to work

From a UKVI point of view, employers need to check, and keep copies of, the documents of prospective employees to ensure that they have the right to work in the UK. Failure to comply with that legal obligation is a criminal offence. The checks must be undertaken by, or on behalf of, the employer prior to employment commencing. Where an employee moves between Trusts in a collaborative bank, the check of documents will need to take place whenever an individual commences work with a new Trust which must then retain copies on file to be relied upon if the individual returns to work at that Trust.

GDPR

As with the ESR Streamlining programme, for the purposes of complying with the GDPR it will be necessary to establish the ways in which personal data is processed through the collaborative bank and also identify the legal basis for processing.

There are six alternative legal bases under Article 6(1) of the GDPR:

(a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose

(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations)

(d) **Vital interests:** the processing is necessary to protect someone's life

(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

(f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests

Consent

Consent has historically been relied upon by employers as the legal basis for processing personal data. However, there has been some debate about how appropriate it is to rely on consent in an employment context (which would include bank work) due to the unequal bargaining position which exists between most employees/workers and their employers and guidance from the Information Commissioner's Office (ICO) has suggested that an alternative basis should be relied on where possible.

Contract

Much of the data processed about workers on a collaborative bank will be used in order to comply with the terms of their contract. For example, the payment of salary to a worker, and therefore the processing of data regarding their bank account details, is necessary so as to comply with the terms of engagement.

Legal obligation

Where organisations are required by law to collect and process certain information, such as an individual's right to work in the UK or to deduct income tax and National Insurance contributions, this will fall under the legal basis of 'legal obligation'. In addition, a worker's rights, such as those under the Working Time Regulations 1998 require that employers collect information about working hours, rest breaks and annual leave to ensure that they are complying with their legal obligations.

Legitimate interests and public tasks

Legitimate interests can be an organisation's own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits. GDPR specifically identifies processing employee/worker data as an example of employer's legitimate interests. A public authority can only rely on 'legitimate interests' if it is processing data for a legitimate reason ***other*** than performing its tasks as a public authority. Unhelpfully, the phrase 'performance of its tasks' is not defined and there has, as yet, been no further guidance issued on this point.

One approach to this issue is to take the view that an NHS organisation is carrying out a public task when it provides health care services and that employment matters fall outside its public task. This is certainly consistent with the approach we take with judicial review where employment matters are a private function of an NHS body and not a public function. It follows that public authorities should be able to take the view that processing matters related to staffing fall under 'legitimate interests'.

Where 'legitimate interests' is relied upon, the organisation must show that its interest is significant enough to override the individual rights of the employee.

The alternative approach would be to view engaging collaborative bank staff as part and parcel of the exercise of the public body's functions, in which case the legitimising condition would be article 6(1)(e).

When a collaborative bank is established, HR should carry out an audit of the personal data which is processed in the operation of the bank and identify for each process the legal basis which applies.

Privacy/Fair Processing Notice

Under the GDPR, Trusts need to explain the lawful basis for processing the personal data of individuals, the likely data retention periods and that staff have a right to complain to the ICO if they think there is a problem with the way their data is being handled. We recommend that this is set out in a specific document, called a privacy notice (or 'fair processing notice').

Privacy notices must contain the following information:

- Identity and contact details of the data controller
- Contact details of the Data Protection Officer (DPO)
- The legal basis for processing the data
- The categories of personal data to be processed
- The recipients of the data
- Whether data will be transferred outside the EU
- Period of storage
- The rights of the data subject
- The existence of any automated decision making

We recommend that each collaborative bank provides workers who are registered with a privacy notice specific to bank work through the collaborative bank.

Summary

Trusts should be advised that, where applicable, they should include e-rostering and collaborative bank work when identifying the means of processing worker and employee data in their HR personal data audit. This will help Trusts to establish the legal basis for processing data under the GDPR and whether data processing contracts with third parties are required.

In establishing a collaborative bank, many of the GDPR considerations which are relevant to the streamlining programme will apply. Collaborative banks take many forms and so specific GDPR advice will need to sought on a case by case basis. However, the principles set out above regarding the legal basis for processing data and the privacy notice will apply across the board.

If you require further assistance with the GDPR impact on both e-rostering and collaborative banks, please contact Nicola Green on 020 780 6975.

Capsticks Solicitors LLP
April 2018