**MILS ADVICE NOTE - GDPR – PREPARATION FOR EMPLOYERS**

**Introduction**

The GDPR represents the biggest change in data protection laws for 20 years. There are a number of points for HR professionals to consider, both in preparing for the GDPR and implementing its provisions from May 2018 onwards.

In section 1 below we look at some general background pointers regarding the GDPR before going on to look, in section 2, at specific employment issues which have been addressed under the ICO Employment Code of Practice “the Code”.

**Section 1: General Pointers: Preparation For The GDPR**

**(a) Awareness**

The GDPR seeks to put data protection at the centre of the business decision making, rather than, as has often become the case under the Data Protection Act 1998, something of a side issue in employment law.

It is important that awareness of the GDPR is from the top down and that the Directors and the Board understand the new regime and the implications. Clearly the potential sanctions under GDPR are greatly increased in terms of fines on potential criminal liabilities, which should be enough to make Directors sit up and take notice. If you are an HR professional, it is likely to fall upon you to be able to summarise the new provisions to the Board. The ICO guidance and commentary suggests that, certainly in the first few years, employers who try to do something (not nothing) and attempt to comply will be treated far more leniently in terms of any data breaches than businesses who have simply ignored the provisions.

**(b) Address the lawful basis for processing data under GDPR for your employees**

(i) What is processing?

Processing is defined under the GDPR at Article 4(2) as:

*“Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”*

As such whenever you are collecting, organising, structuring, storing, adapting, altering, retrieving disseminating or making available personal details, such as an employee’s details for payroll or for a health assessment, then you will need to be complying with the GDPR.

(ii) Lawful?

To comply with the GDPR processing must be lawful. Following Article 6 of the GDPR processing is only lawful if one of the following apply:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

(iii) Why is the lawful ground for processing important?

Whilst consent to any processing will be lawful, which ground you use is very important as the lawful reason for processing any data will affect:

* the legitimate uses to which the data can be put;
* how long it can reasonably be kept; and
* whether the data subject can request for the processing to be stopped, modified and/or deleted.

Whilst you can rely on consent at all times, consent can be withdrawn. Where you are processing data for billing purposes for example it would be more appropriate to rely on ground (b). Where you are keeping the data to comply with FCA regulations for record keeping only ground (c) would be more appropriate.

(iv) Where *must* I rely on consent?

Under the GDPR you *must* rely on consent where you are processing ‘sensitive personal data’.

Sensitive personal data includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The Information Commissioner’s Office have stated that where there is a significant imbalance in power, such as the employer/employee relationship, there will be significant difficulties in relying on consent (save in very specific areas as above where specific consent may be obtained), and that an employer may be better off relying upon the lawful processing categories in (b), (c), (d) and (f) above in respect of employee data. In practice there are significant benefits in this approach.

The trick will be to correctly communicate the grounds to your employees. We have created a template data protection policy under GDPR for clients to use and adapt which follows lawful grounds for processing other than consent.

**(c) Review of contracts and policies**

The GDPR will mean HR need to review and if necessary update employment law and HR documentation that you hold. In particular the following may be considered (not an exhaustive list):

i. If you are not relying on consent under the GDPR, but have previously done so in contracts of employment under the Data Protection Act 1998, such clauses will probably need to be removed from contractual documentation for new starters and with those employees who have existing clauses, specific communications given by the employer making clear that you are no longer relying on consent (under clause X of their contract) but setting out the new basis upon which day the data is being held and processed and referring to your new policies.

ii. You will need to update your data protection policies and references to the new requirements and if necessary introduce a new data protection policy that is compliant with the GDPR.

iii. You may need to consider new documents or amendments to existing documents such as your privacy notice.

iv. There are changes to the processing requirements for Subject Access Requests under the GDPR so if you have particular policies or procedures relating to Subject Access Requests they will need to be updated.

v. Many employers are putting together a firm data breach plan. Under the GDPR there are strict requirements for reporting data breaches, so it is important that serious breaches are flagged and reported in the proper way.

vi. Particular problem areas with data security in the employment law context can arise from homeworking and where data is transferred out of the office so IT may need to review regarding protections, encryption etc.

vii. Other Policies: As set out below in the ICO guidance some particular areas of employment (e.g. recruitment records, monitoring and health records) will need consideration and may need review. Breaches of the GDPR or data protection policies may also need to be highlighted as more serious offences under the disciplinary procedures than previously would have been the case under the Data Protection Act.

viii. Third Party Contracts: Be aware of areas where data is processed by third parties especially matters such as payroll. Appropriate protections/clauses etc may need to be agreed in contracts with third party businesses who contract with the employer.

**(d) Data Protection Officer?**

The position on whether you need a Data Protection Officer is unclear. The GDPR requires one where your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or large-scale processing of special categories of sensitive data such as health records or criminal convictions.

The current wording of the Data Protection Bill requires all data processors to appoint a Data Protection Officer. If this wording passes as law, then a Data Protection Officer may be required under the UK legislation even where one would not be required under the European GDPR.

It is arguable whether, for a normal employer in the motor industry, a Data Protection Officer is mandatory. Many employers are in any event appointing a Data Protection Officer or if not, then the duties needed to ensure compliance with the GDPR are being given to a dedicated manager, to ensure compliance and responsibility on an ongoing basis.

**(e) Training and keeping compliant**

The GDPR is aimed very much at the active consideration in the business of data security, so it is important that businesses keep compliant and don’t just leave matters after initial steps are taken to prepare for May 2018. This could involve regular training of directors and managers and keeping compliant over the years e.g. internal audits. Keep good paper trails so that the business can show to any investigation or complaint that it took reasonable steps to protect data and comply with GDPR.

**Section 2: Specific Areas Of The Employment Relationship To Consider**

In addition to the DPA itself the ICO has published an Employment Code of Practice (“the Code”). This will continue to be relevant under the GDPR. It deals with the following issues:

* Recruitment and selection
* Employment Records
* Monitoring
* Health Records

The Code does not have the force of law itself, but it will be used by the ICO in assessing whether a data controller is processing employee data in accordance with the DPA and GDPR.

The ICO places emphasis on the fact that the Code seeks to create a balance between the needs of the employer and the employee and in order to facilitate this it aims to create a culture of openness in the recruitment and selection process.

The Code is a lengthy document and the ICO has some supplementary guidance which runs to nearly as many pages. A good starting point for the practitioner in this area is the Quick Guide to the Employment Practices Code which is also published by the ICO and set out below are some extracts from this guide.

**2.1 Recruitment and Selection**

This section of the Code applies to the collection and/or use of information about individuals as part of a recruitment or selection exercise, for example the completion of an application form or the receipt of a CV.

Practical Steps to take

To ensure compliant collection and/or use of information the ICO suggests the following steps:

i. Make sure that when you place a recruitment advert you identify your organisation properly. If you are using a recruitment agency, make sure the agency identifies itself.

ii. Use the information you collect for recruitment or selection only. If you are going to use the information for any purpose that goes beyond this, such as to add names to your company’s marketing list, you must explain this clearly.

iii. Ensure that those involved in recruitment and selection are aware that data protection rules apply and that they must handle personal information with respect.

iv. Do not collect more personal information than you need. It is a breach of data protection rules to collect personal information that is irrelevant or excessive. Design your application forms with this in mind.

v. Do not collect from all applicants information that you only need from the person that you go on to appoint, such as banking details, or information you only need from applicants for particular jobs, such as details of motoring offences.

vi. Keep the personal information you obtain secure; it should not normally be disclosed to another organisation without the individual’s consent.

vii. Only ask for information about criminal convictions if this is justified by the type of job you are recruiting for. Don’t ask for ‘spent’ convictions unless the job is covered by the Exceptions Order to the Rehabilitation of Offenders Act 1974.

viii. If you are going to verify the information a person provides, make sure they know how this will be done and what information will be checked.

ix. If you need to verify criminal conviction information, only do this by getting a ‘disclosure’ about someone from the Criminal Records Bureau (CRB). Make sure you are entitled to receive this information and that you follow the CRB’s procedures strictly. Only keep a record that a satisfactory/unsatisfactory check was made; do not hold on to detailed information.

x. Only keep information obtained through a recruitment exercise for as long as there is clear business need for it.

**2.2 Employment Records**

The GDPR will generally apply to any information an employer keeps about its workers with the emphasis on creating a balance between the needs of employer and employee and also ensuring openness. The ICO suggests the following practical steps.

Practical Steps to take

i. You don’t need to get the consent of workers to keep records about them, but make sure they know how you will use records about them and whether you will disclose the information they contain.

ii. Ensure that those who have access to employment records are aware that data protection rules apply, and that personal information must be handled with respect.

iii. Check what records are kept about your workers, and make sure you are not keeping information that is irrelevant, excessive or out of date. Delete information that you have no genuine business need for or legal duty to keep.

iv. Be careful when disclosing information in the worker’s employment record. Remember that those asking for information about workers may not actually be who they claim to be.

v. Data protection doesn’t stand in the way where you are legally obliged to disclose information, for example informing the Inland Revenue about payments to workers. You should nevertheless be careful not to disclose more information than required.

vi. In some cases, you will not be legally obliged to disclose but you will be able to rely on an exemption in the Data Protection Act if you choose to do so. This is most likely to apply in criminal or tax investigations or where legal action is involved. You will still need to take care if confidential or other sensitive information is involved.

vii. In other cases, you could breach the Act if you disclose. Only disclose if, in all the circumstances, you are satisfied that it is fair to do so. Bear in mind that fairness to the worker should be your first consideration.

viii. Don’t provide a confidential reference or similar information about a worker unless you are sure that the worker would agree to this. If in doubt, ask the worker concerned.

ix. Let workers check their own records periodically. This will allow mistakes to be corrected and information to be kept up to date.

x. Keep employment records secure. Keep paper records under lock and key and use password protection for computerised ones. Make sure that only staff with proper authorisation and the necessary training have access to employment records.

xi. Where possible, keep sickness records containing details of a worker’s illness or medical condition, separate from other less sensitive information, for example a simple record of absence. This can be done by keeping the sickness record in a sealed envelope or in a specifically protected computer file. Only allow managers access to health information where they genuinely need it to carry out their job.

xii. If you collect information about workers to administer a pension or insurance scheme, only use the information for the administration of the scheme. Make sure workers know what information the insurance company or other scheme provider will pass back to you as the employer.

xiii. If you collect sensitive information to help monitor equal opportunities, for example about workers’ disabilities, race or sexuality, only use the information for that purpose. Where possible use anonymised information, that is information that does not allow particular workers to be identified.

xiv. If you intend to use the information you keep about workers to send marketing material to them, give them a chance to opt out before doing so. If you intend to pass on their details to another organisation for its marketing, then get the worker’s positive agreement before doing so (that is, you should ask them to indicate that they do agree, rather than assuming they agree unless they say they don’t).

xv. When you no longer have a business need or legal requirement to keep a worker’s employment record, make sure it is securely disposed of, for example by shredding it.

**2.3 Monitoring at Work**

Where an employer monitors his workers by collecting or using information about them then the GDPR will apply to ensure a climate of openness and balance of the parties’ needs. Practical steps suggested by the ICO are the following:

Practical Steps to take

i. Consider why you want to carry out the monitoring. This might mean asking what problem you are trying to solve, for example theft in the workplace.

ii. Once you are clear about the purpose, ask whether the particular monitoring arrangement will truly bring the benefit you are looking for and whether it is justified by this benefit.

iii. Remember:

* Monitoring is usually intrusive;
* Workers legitimately expect to keep their personal lives private;
* Workers are entitled to some privacy in the work environment.

iv. Consider whether alternative approaches or different methods of monitoring would deliver the benefits you want while being more acceptable to workers. Can you target the monitoring at an area of risk, for example the part of your premises where you think theft is occurring?

v. Ensure your workers are aware that they are being monitored and why. You could tell them this by putting a notice on a notice-board or signs in the areas where monitoring is taking place. If your workers have computers, you could send them an email about the monitoring. If you are open about it, they will know what to expect.

vi. If monitoring is to be used to enforce your rules and standards, make sure workers know clearly what these are.

vii. Only use information obtained through monitoring for the purpose for which you carried out the monitoring, unless the monitoring leads to the discovery of an activity that no employer could reasonably be expected to ignore, for example breaches of health and safety rules that put other workers at risk.

viii. Keep secure the information that you gather through monitoring. This might mean only allowing one or two people to have access to it. Don’t keep the information for longer than necessary or keep more information than you really need. This might mean deleting it once disciplinary action against a worker is over.

For particular types of monitoring the following should be considered:

i. Be particularly careful when monitoring communications, such as emails, that are clearly personal. Avoid wherever possible opening emails, especially those that clearly show they are private or personal. Monitor the message’s address or heading only.

ii. If it is necessary to check the email accounts or voicemails of workers in their absence, make sure they are aware this will happen.

iii. Where video or audio monitoring is justified, target the monitoring, where possible, at areas of particular risk, and only use it where workers wouldn’t expect much privacy.

iv. Ensure that if you use information for monitoring which is held by third parties, such as credit reference or electoral roll information, you can justify this. Take particular care with any information you hold about workers as a result of non-employment dealings with them, for example where they are also your customers.

v. If you are justified in obtaining information about a worker’s criminal convictions for monitoring, only do so through a ‘disclosure’ from the Criminal Records Bureau.

vi. If you monitor workers through information held by a credit reference agency, you must tell the agency what you will use the information for. Do not use a facility for carrying out credit checks on customers to monitor or vet workers.

If intending to carry out covert monitoring, then the ICO suggests that the following should be considered:

i. The covert monitoring of workers can rarely be justified. Do not carry it out unless it has been authorised at the highest level in your business. You should be satisfied that there are grounds for suspecting criminal activity or equivalent malpractice, and that telling people about the monitoring would make it difficult to prevent or detect such wrongdoing.

ii. Use covert monitoring only as part of a specific investigation and stop when the investigation has been completed. Do not use covert monitoring in places such as toilets or private offices unless you suspect serious crime and intend to involve the police.

Also relevant in this area are the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (“LBPs”).

The LBPs were created pursuant to RIPA and came into force on 24th October 2000 and set out the circumstances in which public and private bodies may make lawful interceptions.

This has particular relevance within an employment context. In this case an interception of an employee’s communication by his employer may take place without consent if it is for the following purposes:-

Monitoring and recording is permitted in the following circumstances:-

i. the prevention or detection of crime, including fraud.

ii. the investigation or detection of unauthorised use of the system.

iii. the establishment of facts relevant to the business.

iv. to verify compliance with regulatory practices or procedures that are relevant to the business.

v. to verify or demonstrate that employees are using the system to an appropriate standard.

vi. to ensure effective operation of the system.

Monitoring solely is permitted without consent if:-

i. it is undertaken to determine whether received communications are relevant to the employer’s business; or

ii. it is undertaken to identify calls being made to counselling or support help lines.

Note that “relevant to the employer’s business” is defined as a communication:

a. by means of which a transaction is entered into in the course of that business; or

b. which otherwise relates to that business; or

c. communication which otherwise takes place in the course of the carrying on of that business.

**2.4 Information about Worker’s Health**

The GDPR will apply to any collection or use of information by an employer about his workers’ health, for example in the case of a questionnaire or where a worker is tested for drugs or alcohol use.

It is important to note that the collection and use of health information brings the GDPR rules on sensitive personal data into play and therefore care must be taken to ensure that the employer is clear about why he is doing this and is satisfied that his action is justified by the benefits that will result.

The ICO makes the following recommendations:-

Practical Steps to take

i. Consider why you want to collect and use this information. This might mean identifying a problem you are trying to solve, for example work that is impaired due to drug or alcohol use.

ii. Make sure that you can satisfy a sensitive data condition. You are most likely to do this if:

 a. collecting health information is necessary to protect health and safety; or

 b. the collection is necessary to prevent discrimination on the grounds of disability; or

 c. each worker affected has given explicit consent.

iii. Bear in mind that if you rely on consent it must be freely given. This means a worker must be able to say “no” without a penalty being imposed and must be able to withdraw consent once given. A person is more likely to be in this position at the recruitment stage than when they are employed.

iv. Once you are clear about the purpose and that you can satisfy a sensitive data condition, check that the collection and use of health information is justified by the benefits that will result. In doing so, remember that:

 a. gathering information about your workers’ health will be intrusive, perhaps highly intrusive;

 b. workers can legitimately expect to keep their personal health information private and expect that employers will respect this privacy.

v. Consider whether alternative ways of collecting information about your workers’ health would deliver the benefits you want while being more acceptable to them. For example, you might use health questionnaires rather than medical testing or at least use a questionnaire to select those to be tested.

vi. Collect information about as few workers as possible. Collect health information in areas of highest risk only; in other words, consider whether you can involve only a few individuals whose jobs are critical to safety or who work in a hazardous environment.

vii. Keep information about workers’ health particularly secure. This might mean allowing only one or two people to have access to it, for example by password-protecting it, or keeping it in a sealed envelope in a worker’s file.

viii. Don’t keep information for longer than necessary or collect more information than you really need. This might mean deleting medical details once disciplinary action against a worker is over.

ix. Remember that, as an employer, your interest is mainly in knowing whether a worker is or will be fit to work. As far as possible it should be left to doctors and nurses to have access to and interpret detailed medical information for you.

x. Let your workers know that information about their health is being collected and why. You could give out general information about this by putting a notice on a notice board or sending a letter to workers. If your workers have computers, you could send them an email about it.

xi. Where you are taking specific action, for example where a worker is to undergo a medical test, ensure the worker is fully aware what, why and how much information is to be collected. Be particularly careful that if they are referred to a doctor or nurse, they know what sort of information you will receive as a result.

Additional points to bear in mind when collecting information through drug and alcohol testing:

i. Collecting information by testing workers for drug or alcohol use is usually justifiable for health and safety reasons only.

ii. Where testing is used to enforce the business’ rules and standards, make sure the rules and standards have been clearly set out to workers. Follow these guidelines.

* Only use drug or alcohol tests where they provide significantly better evidence of impairment than other less intrusive means.
* Use the least intrusive forms of testing that will bring the intended benefits to the business.
* Tell workers what drugs they are being tested for.
* Base any testing on reliable scientific evidence about the effect of particular substances on workers.
* Limit testing to those substances and the extent of exposure that will meet the purpose(s) for which the testing is conducted.
* Ensure random testing is genuinely random. It is unfair and deceptive to let workers believe that testing is random if, in fact, other criteria are being used.
* Do not collect personal information by testing all workers, whether randomly or not, if only workers carrying out a particular activity pose a risk. Workers in different jobs will pose different safety risks, so the random testing of all workers will rarely be justified.

**Conclusion**

In conclusions, whilst the GDPR will bring with it challenges and change, the intention is to update data protections and processes, not reinvent them. Many requirements can be seen as best practice and should result in a data policies and processes that better fit the requirements of a modern employer.

Don’t forget, this advice is general in nature. As a MILS member you have access to legal professional who specialize in employment law within the motor industry. Should you need any further advice and guidance please contact us.