Expert-RoadCraft

Expert Driving is no Accident

Policy—data protection

You must read this policy because it gives important information about:

- the data protection principles with which the Company must comply;
- what is meant by personal data (or information) and special category data (or information);
- how we gather, use and (ultimately) delete personal data and special category data in accordance with the data protection principles;
- where more detailed privacy information can be found, eg about the personal data we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that data secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

Once you have read and understood this policy, please confirm you that have done so by signing and returning the attached copy to **[**the data protection officer OR [*insert job title or department*]**]**.

1 Introduction

1.1 The Company obtains, keeps and uses personal data (also referred to as personal information) about job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices for a number of specific lawful purposes, as set out in the Company's [*data protection privacy notices relating to recruitment and employment*].

Paragraph **1.1**—Lawful purposes**:**

ICO guide to the UK GDPR: Lawful basis for processing—how do we decide which lawful basis applies?

Employers must determine their lawful basis for processing before starting to process personal data. According to the ICO guidance, it is important to get this right first time; retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.

The Precedent envisages that the employer will take a layered approach and refer to the relevant privacy notice in the policy. See eg Precedents:

(a) Data protection privacy notice (recruitment)

(b) Data protection privacy notice (employment)

(c) Data protection privacy notice (secondment—employer to employee)

(d) Data protection privacy notice (TUPE transfer)

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal data relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal data relating to our workforce, and how (and when) we delete that data once it is no longer required.

Paragraph **1.3**—Transparency**:**

Articles 5(1)(a), 12 of Assimilated Regulation (EU) 2016/679, UK GDPR

Employers are required to take appropriate measures to provide information about processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

For more detailed information, see Practice Note: Data protection privacy notices—issues in employment.

1.4 **[**The Company's data protection officer, [*insert name*], is responsible for informing and advising the Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Company's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer [*set out details of how DPO can be contacted, eg email and telephone number*].

OR

1.5 [*Insert job title or department*] is responsible for data protection compliance within the Company. If you have any questions or comments about the content of this policy or if you need further information, you should contact [*insert job title or department*] [*set out details of how individual/department can be contacted, eg email and telephone number*].**]**

Paragraphs **1.4** or **1.5**—Data protection responsibility**:**

Articles 37–39 of Assimilated Regulation (EU) 2016/679, UK GDPR

An employer, as a controller, must appoint a DPO if:

(a) it is a public authority or body (there is an exception for courts acting in their judicial capacity)

(b) its core activities consist of large-scale systematic monitoring of individuals, for example, businesses engaging in online profiling or behaviour tracking, or

(c) its core activities consist of large-scale processing of special category data, or data relating to criminal convictions and offences

Businesses not subject to this requirement may still decide to appoint a DPO in order to manage the organisation's data protection framework and as a matter of good practice.

For further information, see Practice Note: Data protection officer and Precedent: Data protection officer—DPO—job description and role profile.

2 Scope

2.1 This policy applies to the personal data of job applicants and current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices.

Paragraph **2.1**—Scope**:**

It is likely that an employer will need to process certain personal data relating to job applicants during the recruitment process. Once an individual has been recruited, certain of the data gathered during the recruitment process will no longer be required but other, additional data will be required (eg bank details and PAYE information). This will be the case for employees and other workers, both during the employment relationship and afterwards.

For a sample data protection privacy notice for use:

(a) in relation to job applicants and prospective employees and other workers, see Precedent: Data protection privacy notice (recruitment)

(b) in relation to employees and other workers, see Precedent: Data protection privacy notice (employment)

For a supplemental privacy notice for use where an employee is going on secondment, see Precedent: Data protection privacy notice (secondment—employer to employee). Precedent: Data protection privacy notice (employment) can be adapted for use by the host employer.

2.2 Staff should refer to the Company's [*data protection privacy notice*] and, where appropriate, to its other relevant policies including in relation to [*internet, email and communications, monitoring, social media, information security, data retention, bring your own device (BYOD) and criminal record information*], which contain further information regarding the protection of personal data in those contexts.

Paragraph **2.2**—Other relevant policies**:**

The Precedent envisages that the employer will take a layered approach and refer to the privacy notice and other relevant policies in this policy. See the list of sample Precedents set out above.

2.3 **[**This policy has been drafted with the assistance of a representative group of employees to ensure that it is clear and easy to understand. **]**We will review and update this policy [*regularly*] in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff **[**before OR when**]** it is adopted.

Paragraph **2.3**—Status and updating of policy**:**

Articles 35(2), (9) of Assimilated Regulation (EU) 2016/679, UK GDPR

While there is no obligation on the employer to seek employees' views on the policy (as there is in respect of a data protection impact assessment), it is probably good employment practice to do so, particularly to ensure that it is clear and intelligible to all employees.

DPA 2018, Sch 1 Pt 4, paras 38(1), 40(1), 40(2)

The employer must (from when it starts to carry out the processing of personal data until six months after it ceases to carry out such processing):

(a) keep the policy document under review and updated, and

(b) make it available to the Information Commissioner on request

ICO guide to the UK GDPR: Accountability and governance—Documentation

ICO guidance also suggests that it is good practice for employers to conduct regular reviews of the personal data they process and update their documentation accordingly.

3 Definitions

criminal records data	means personal data relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
data subject	means the individual to whom the personal data relates;
personal data	(sometimes known as personal information) means data relating to an individual who can be identified (directly or indirectly) from that data;
processing data	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying data, or using or doing anything with it;
pseudonymised	means the process by which personal data is processed in such a way that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual;
special category data	(sometimes known as 'special categories of personal data', 'sensitive personal data' or 'sensitive personal information') means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics data, biometric data (where used to identify an individual) and data concerning an individual's health, sex life or sexual orientation.

Paragraph Error! Reference source not found.—Definitions**:**

Article 4 of Assimilated Regulation (EU) 2016/679, UK GDPR

The definitions in this paragraph reflect those in Article 4 of Assimilated Regulation (EU) 2016/679, UK GDPR.

DPA 2018, s 11(2)

DPA 2018, s 11(2) clarifies that criminal records data includes personal data relating to allegations and criminal proceedings, including sentencing.

4 Data protection principles

4.1 The Company will comply with the following data protection principles when processing personal data:

4.1.1 we will process personal data lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal data that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;

4.1.5 we will keep personal data**[** in a form which permits identification of data subjects**]** for no longer than is necessary for the purposes for which the data are processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Paragraph **4**—Data protection principles**:**

Article 5 of Assimilated Regulation (EU) 2016/679, UK GDPR

This paragraph is a statement of the Company's compliance with the data protection principles set out in Article 5 of Assimilated Regulation (EU) 2016/679, UK GDPR. See Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—Principles.

5 Basis for processing personal data

5.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, ie:

(a) that the data subject has consented to the processing;

(b) that the 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) that the processing is necessary for compliance with a legal obligation to which the Company is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;**[** or**]**

(e) **[**that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or**]**

(f) that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 5.2 below.

5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (ie that there is no other reasonable way to achieve that purpose);

5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

5.1.5 where 'special category data is processed, also identify a lawful special condition for processing that data (see paragraph 6.2.2 below), and document it; and

5.1.6 where criminal records data is processed, also identify a lawful condition for processing that data, and document it.

Paragraph **5.1**—Compliance checklist**:**

ICO guide to the UK GDPR: Lawful basis for processing

This paragraph, adapted from the ICO guidance, documents the way in which the Company will meet its data protection obligations and also serves as a checklist for the DPO or other person responsible for data protection compliance.

For information on the lawful conditions for processing personal data that are most likely to apply in the employment context, see Practice Note: The UK GDPR and DPA 2018: lawful processing of personal data in employment—Personal data—lawful processing conditions.

Article 6(1)(e) of Assimilated Regulation (EU) 2016/679, UK GDPR

Include the optional paragraph if the organisation is likely to want to rely on Article 6(1)(e) which gives a lawful basis for processing that 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'. While this is unlikely to be relevant in the employment context, if the employer is a public authority or other organisation that exercises official authority or carries out tasks in the public interest it may want the option of relying on this lawful basis for processing.

5.2 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

5.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

5.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

5.2.3 keep the LIA under review, and repeat it if circumstances change; and

5.2.4 include information about our legitimate interests in our relevant privacy notice(s).

Paragraph **5.2**—Legitimate interests checklist**:**

ICO guide to the UK GDPR: Legitimate interests

This paragraph, adapted from the ICO guidance, documents the way in which the Company will ensure that 'legitimate interests' is the appropriate condition for lawful processing, and also serves as a checklist for the DPO or other person responsible for data protection compliance.

See Practice Note: The UK GDPR and DPA 2018: lawful processing of personal data in employment—Lawful condition for processing—legitimate interests.

6 Special category data

6.1 Special category data is sometimes referred to as 'sensitive personal data' or 'sensitive personal information'.

6.2 The Company may from time to time need to process special category data. We will only process special category data if:

6.2.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above, eg it is necessary for the performance of the employment contract, to comply with the Company's legal obligations or for the purposes of the Company's legitimate interests; and

6.2.2 one of the special conditions for processing special category data applies, eg:

(a) the data subject has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

6.3 Before processing any special category data, staff must notify **[**the data protection officer OR [*insert job title or department*]**]** of the proposed processing, in order that **[**the data protection officer OR [*insert job title or department*]**]** may assess whether the processing complies with the criteria noted above.

6.4 special category data will not be processed until:

6.4.1 the assessment referred to in paragraph 6.3 has taken place; and

6.4.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.5 **[**The Company will not carry out automated decision-making (including profiling) based on any individual's special category data.**]**

Paragraph **6.5**—Automated decision-making**:**

As mentioned above, this Precedent assumes that, in the employment context, the employer does not carry out profiling or any other automated decision-making based on special category data.

For further information, see Practice Note: Other data subject rights—issues in employment—Rights related to automated decision-making and profiling.

6.6 The Company's [*data protection privacy notice*] sets out the types of special category data that the Company processes, what it is used for and the lawful basis for the processing.

Paragraph **6.6**—Privacy notice**:**

In keeping with a layered approach, this Precedent directs individuals to Precedent: Data protection privacy notice (employment).

6.7 In relation to special category data, the Company will comply with the procedures set out in paragraphs 6.8 and 6.9 below to make sure that it complies with the data protection principles set out in paragraph 4 above.

6.8 **During the recruitment process**: the HR department, with guidance from **[**the data protection officer OR [*insert job title or department*], will ensure that (except where the law permits otherwise):

6.8.1 during the short-listing, interview and decision-making stages, no questions are asked relating to special category data, eg race or ethnic origin, trade union membership or health;

6.8.2 if special category data is received, eg the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

6.8.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

6.8.4 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

6.8.5 we will **[**not ask health questions in connection with recruitment OR only ask health questions once an offer of employment has been made**]**.

Paragraph **6.8**—Processing special category data during the recruitment process**:**

Equality Act 2010, s 60

Generally, an employer cannot ask health-related questions before an offer of employment is made (or before the employee is put into a pool of applicants who may be offered a vacancy if one comes up). Such questions may only be asked:

(a) to establish whether the applicant will be able to comply with a requirement to undergo an assessment (ie an interview or other selection procedure)

(b) to establish whether a duty to make reasonable adjustments arises in relation to the job applicant's need to undergo an assessment

(c) to establish whether the applicant will be able to carry out a function that is intrinsic to the work concerned

(d) to monitor diversity in the range of persons applying to the prospective employer for work

(e) to take 'positive action' in relation to disabled persons

(f) to establish whether the applicant has a particular disability, in circumstances where the employer requires that any applicant for the work in question has that disability (but only where the criteria necessary for the occupational requirement exception to apply are fulfilled)

The words ' except where the law permits otherwise' are included to allow for those circumstances.

For further information, see Practice Notes: Medical reports—data protection issues and AMRA 1988—Obtaining a medical report before an offer of employment is made—EqA 2010 and Employment events which give rise to discrimination, harassment and victimisation claims—Pre-employment enquiries about disability and health.

6.9 **During employment**: the HR department, with guidance from the data protection officer OR [*insert job title or department*]**]**, will process:

6.9.1 health data for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

6.9.2 special category data for the purposes of equal opportunities monitoring and pay equality reporting**[**. Where possible, this data will be anonymised**]**; and

6.9.3 trade union membership data for the purposes of staff administration and administering 'check off'.

Paragraph **6**—Special category data**:**

For further information on the particular requirements that apply in relation to processing special category data, see Practice Note: The UK GDPR and DPA 2018: lawful processing of personal data in employment—Special category data—specific processing conditions.

Additional safeguards must be fulfilled when processing special category data in reliance on the following specific conditions for processing:

(a) DPA 2018, s 10(2), Sch 1 Pt 1

obligations and rights under employment law (DPA 2018, Sch 1 Pt 1), and

(b) DPA 2018, s 10(3), Sch 1 Pt 2

substantial public interest conditions (DPA 2018, Sch 1 Pt 2)

These include (in the case of obligations and rights under employment law and most substantial public interest conditions) a requirement for the employer to have in place an 'appropriate policy document'. For further information, see the following main sections in Practice Note: The UK GDPR and DPA 2018: lawful processing of personal data in employment:

(a) Special category data—specific processing conditions

(b) Specific condition—obligations and rights under employment law

(c) Specific condition—substantial public interest, and

(d) Appropriate policy document

This data protection policy, together with related policies including Precedents: Policy—records retention (employment) and Records retention schedule (employment), is designed to fulfil these requirements.

7 Criminal records data

Criminal records data will be processed in accordance with the Company's [*Criminal records data policy*].

Paragraph **7**—Criminal records data**:**

For a sample criminal records data policy, see Precedent: Policy—criminal records information.

DPA 2018, s 10(4), (5), Sch 1 Pt 1, Sch 1 Pt 2, Sch 1 Pt 3

In the employment context, DPA 2018, Sch 1 Parts 1 and 2 set out the additional safeguards that must be fulfilled in order for processing of personal data regarding criminal convictions and offences to take place. These include a requirement for the employer to have in place an 'appropriate policy document'. For further information, see Practice Note: Criminal offence data—employment data protection issues. This data protection policy, together with Precedents: Policy— criminal records information, Policy—records retention (employment) and Records retention schedule (employment), is designed to fulfil these requirements.

8 Data protection impact assessments (DPIAs)

8.1 Where processing is likely to result in a high risk to an individual's data protection rights (eg where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

8.1.1 whether the processing is necessary and proportionate in relation to its purpose;

8.1.2 the risks to individuals; and

8.1.3 what measures can be put in place to address those risks and protect personal data.

8.2 Before any new form of technology is introduced, the manager responsible should therefore contact **[**the data protection officer OR [*insert job title or department*]**]** in order that a DPIA can be carried out.

8.3 During the course of any DPIA, the employer will seek the advice of the **[**data protection officer OR [*insert job title or department*]**]** and the views of**[** a representative group of**]** employees and any other relevant stakeholders.

Paragraph **8**—Data protection impact assessments**:**

Data protection impact assessments (DPIAs), also known as 'privacy impact assessments' (PIAs), are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

Recitals 89–91, Article 35(1) of Assimilated Regulation (EU) 2016/679, UK GDPR

An employer must carry out a DPIA when:

(a) using new technologies, and

(b) the processing is likely to result in a high risk to the rights and freedoms of individuals

Articles 35(2), 35(9) of Assimilated Regulation (EU) 2016/679, UK GDPR

The employer must seek the advice of the designated DPO when carrying out a DPIA and, where appropriate, seek the views of the individuals whose personal data will be the subject of the processing, or of their representatives. The policy wording also refers to 'any other relevant stakeholders' in order to give the employer additional flexibility in relation to those it consults.

For further information, see Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—Accountability, under the heading 'Data protection impact assessments'.

9 Documentation and records

9.1 We will keep written records of processing activities**[** which are high risk, ie which may result in a risk to individuals' rights and freedoms or involve special category data or criminal records data**]**, including:

9.1.1 the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);

9.1.2 the purposes of the processing;

9.1.3 a description of the categories of individuals and categories of personal data;

9.1.4 categories of recipients of personal data;

9.1.5 **[**where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;**]**

9.1.6 where possible, retention schedules; and

9.1.7 where possible, a description of technical and organisational security measures.

Paragraph **9.1**—Written records of processing activities**:**

Articles 30(1), 30(3) and 30(5) of Assimilated Regulation (EU) 2016/679, UK GDPR

Include the wording in square brackets if the employer has fewer than 250 employees. In the case of employers with fewer than 250 employees, the requirement to keep written records applies only where:

(a) the processing is likely to result in a risk to the rights and freedoms of data subjects

(b) the processing is not occasional, or

(c) the processing includes special categories of data or personal data relating to criminal convictions and offences

However, it is good practice to keep written records of processing activities and all employers should consider doing so, regardless of size. See Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—Accountability, under the heading 'Records of processing activities' and Precedent: Data processing register.

9.2 As part of our record of processing activities we document, or link to documentation, on:

9.2.1 information required for privacy notices;

9.2.2 records of consent;

9.2.3 controller-processor contracts;

9.2.4 the location of personal data;

9.2.5 DPIAs; and

9.2.6 records of data breaches.

9.3 If we process special category data or criminal records data, we will keep written records of:

9.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

9.3.2 the lawful basis for our processing; and

9.3.3 whether we retain and erase the personal data in accordance with our policy document and, if not, the reasons for not following our policy.

Paragraph **9.3**—Records of sensitive personal data processing**:**

DPA 2018, Sch 1 Pt 1, para 1, Sch 1 Pt 4, para 41

The employer's data processing records must include information on:

(a) which condition is relied on

(b) the lawful basis on which processing takes place, and

(c) whether the personal data is retained and erased in accordance with the appropriate policy document and if not, the reasons for not following those policies

See Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—Accountability, under the heading 'Records of processing activities' and Precedents: Policy—records retention (employment) and Records retention schedule (employment).

9.4 We will conduct regular reviews of the personal data we process and update our documentation accordingly.**[** This may include:**]**

9.4.1 **[**carrying out data audits to find out what personal data the Company holds;

9.4.2 distributing questionnaires and talking to staff across the Company to get a more complete picture of our processing activities; and

9.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.**]**

Paragraph **9.4**—Regular reviews**:**

ICO guide to the UK GDPR: Accountability and governance—documentation

The wording in square brackets sets out the 'best practice' suggestions provided in the ICO guidance on accountability and governance. See subtopic: Data mapping—overview.

9.5 **[**We document our processing activities in electronic form so we can add, remove and amend data easily.**]**

Paragraph **9**—Documentation and records**:**

ICO detailed guidance: The right to be informed

The wording in this clause reflects a layered approach to the documentation requirements, in keeping with the ICO guidance.

Article 30(1) of Assimilated Regulation (EU) 2016/679, UK GDPR

As well as an obligation to provide comprehensive, clear and transparent privacy statements, if an employer has 250 or more employees, it must maintain additional internal written records of its processing activities.

Article 30(3) of Assimilated Regulation (EU) 2016/679, UK GDPR

An employer with fewer than 250 employees is only required to maintain written records of activities related to higher-risk processing, such as:

(a) processing personal data that could result in a risk to the rights and freedoms of data subjects

(b) processing is not occasional, or

(c) processing of special category data or criminal convictions and offences

However, it is good practice to keep written records of processing activities and all employers should consider doing so, regardless of size. See Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—Accountability, under the heading 'Records of processing activities' and Precedent: Data processing register.

Article 30(1) of Assimilated Regulation (EU) 2016/679, UK GDPR

Affected employers must record:

(a) the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO)

(b) the purposes of the processing

(c) a description of the categories of individuals and the categories of personal data

(d) the categories of recipients of personal data

(e) details of transfers of personal data to third countries or international organisations, including the transfer mechanism safeguards in place

(f) retention schedules (where possible)

(g) Article 32(1) of Assimilated Regulation (EU) 2016/679, UK GDPR

a description (where possible) of the technical and organisational security measures that the employer has taken (appropriate to the level of risk) to ensure that personal data is kept secure

10 Privacy notice

10.1 The Company will issue privacy notices from time to time, informing you about the personal data that we collect and hold relating to you, how you can expect your personal data to be used and for what purposes.

10.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Paragraph **10**—Privacy notices**:**

Articles 12–14 of Assimilated Regulation (EU) 2016/679, UK GDPR

Employers are required to take 'appropriate measures' to ensure that information about the processing of personal data is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

For further information, see Practice Note: Data protection privacy notices—issues in employment, and Precedents: Data protection privacy notice (employment) and Data protection privacy notice (recruitment).

11 Individual rights

11.1 You (in common with other data subjects) have the following rights in relation to your personal data:

11.1.1 to be informed about how, why and on what basis that data is processed—see the Company's [*data protection privacy notice*];

Paragraph **11.1.1**—Right to be informed**:**

Articles 12(1), 13, 14 of Assimilated Regulation (EU) 2016/679, UK GDPR

The 'right to be informed' is a controller's obligation to provide 'fair processing information', typically through a privacy notice, to the individuals whose personal data is being processed. Controllers are expected to take 'appropriate measures' to ensure that the information provided to people about how they process personal data is:

(a) concise, transparent, intelligible and easily accessible

(b) written in clear and plain language, particularly if addressed to a child, and

(c) free of charge

For further information, see Practice Note: Data protection privacy notices—issues in employment, and Precedents: Data protection privacy notice (recruitment), Data protection privacy notice (employment) and Data protection privacy notice (secondment—employer to employee).

11.1.2 to obtain confirmation that your data is being processed and to obtain access to it and certain other information, by making a data subject access request—see the Company's subject access request policy;

Paragraph **11.1.2**—Right to make a data subject access request**:**

Recital 63, Articles 12, 15 of Assimilated Regulation (EU) 2016/679, UK GDPR

Individuals have the right to obtain:

(a) confirmation that their data is being processed

(b) access to their personal data, and

(c) other supplementary information—this largely corresponds to the information that should be provided in a privacy notice

For further information, see Practice Note: Data subject access requests—issues in employment and Precedent: Policy—data subject access requests.

11.1.3 to have data corrected if it is inaccurate or incomplete;

11.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

Paragraphs **11.1.3** and **11.1.4**—Right to rectification and erasure**:**

Articles 12, 16, 19 of Assimilated Regulation (EU) 2016/679, UK GDPR

Individuals have the right to obtain:

(a) confirmation that their data is being processed

(b) access to their personal data, and

(c) other supplementary information—this largely corresponds to the information that should be provided in a privacy notice

For further information, see Practice Note: Other data subject rights—issues in employment—The right to rectification.

Articles 12, 17, 19 of Assimilated Regulation (EU) 2016/679, UK GDPR

Individuals also have the right to request the deletion or removal of personal data where there is no compelling reasons for its continued processing. For further information, see Practice Note: Other data subject rights—issues in employment—The right to erasure (right to be forgotten).

11.1.5 to restrict the processing of personal data where the accuracy of the data is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal data but you require the data to establish, exercise or defend a legal claim; and

11.1.6 to restrict the processing of personal data temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

Paragraphs **11.1.5** and **11.1.6**—Right to restrict processing**:**

Recital 67, Articles 18, 19 of Assimilated Regulation (EU) 2016/679, UK GDPR

Individuals have the right to 'block' or suppress processing of personal data. An employer must restrict the processing of personal data:

(a) where the individual contests the accuracy of the personal data, until the employer has verified the accuracy of the personal data

(b) when processing is unlawful, but the individual opposes erasure and requests restriction instead

(c) if the employer no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

(d) where the individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the employer is considering whether the organisation's legitimate grounds override those of the individual

When processing is restricted, employers are permitted to store the personal data, but not further process it. The employer can retain just enough data about the individual to ensure that the restriction is respected in future.

For further information, see Practice Note: Other data subject rights—issues in employment—The right to restrict processing.

11.2 If you wish to exercise any of the rights in paragraphs 11.1.3 to 11.1.6, please contact **[**the data protection officer OR [*insert job title or department*]**]**.

12 Individual obligations

12.1 Individuals are responsible for helping the Company keep their personal data up to date. You should let [*the HR department*] know if the data you have provided to the Company changes, for example if you move house or change details of the bank or building society account to which you are paid.**[** Alternatively, you can update your own personal data on a secure basis via the Company's intranet.**]**

12.2 You may have access to the personal data of other members of staff, suppliers and **[**customers OR clients**]** of the Company in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 11.1 above.

12.3 If you have access to personal data, you must:

12.3.1 only access the personal data that you have authority to access, and only for authorised purposes;

12.3.2 only allow other Company staff to access personal data if they have appropriate authorisation;

12.3.3 only allow individuals who are not Company staff to access personal data if you have specific authority to do so from **[**the data protection officer OR [*insert job title or department*]**]**;

12.3.4 keep personal data secure (eg by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Company's [*information security policy*]);

Clause **12.3.4**—Information security**:**

This Precedent envisages that policy wording on keeping personal data will be set out in a separate policy. See Precedent: Policy—information security.

12.3.5 not remove personal data, or devices containing personal data (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the data and the device; and

12.3.6 not store personal data on local drives or on personal devices that are used for work purposes**[**, and comply with the Company's [*BYOD policy*]**]**.

12.4 You should contact **[**the data protection officer OR [*insert job title or department*]**]** if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

12.4.1 processing of personal data without a lawful basis for its processing or, in the case of special category data, without one of the conditions in paragraph 6.2.2 being met;

12.4.2 any data breach as set out in paragraph 15.1 below;

12.4.3 access to personal data without the proper authorisation;

12.4.4 personal data not kept or deleted securely;

12.4.5 removal of personal data, or devices containing personal data (or which can be used to access it), from the Company's premises without appropriate security measures being in place;

12.4.6 any other breach of this policy or of any of the data protection principles set out in paragraph 4.1 above.

13 Information security

13.1 The Company will use appropriate technical and organisational measures**[** in accordance with the Company's **[**policies OR information security policy**]]** to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

13.1.1 making sure that, where possible, personal data is pseudonymised or encrypted;

13.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

13.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner; and

13.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Paragraph **13.1**—Integrity and confidentiality**:**

Articles 5(1)(f), 32 of Assimilated Regulation (EU) 2016/679, UK GDPR

This paragraph sets out the Company's commitment to the sixth data protection principle, that personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

13.2 Where the Company uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. In particular, contracts with external organisations must provide that:

13.2.1 the organisation may act only on the written instructions of the Company;

13.2.2 those processing the data are subject to a duty of confidence;

13.2.3 appropriate measures are taken to ensure the security of processing;

13.2.4 sub-contractors are only engaged with the prior consent of the Company and under a written contract;

13.2.5 the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights in relation to data protection;

13.2.6 the organisation will assist the Company in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

13.2.7 the organisation will delete or return all personal data to the Company as requested at the end of the contract; and

13.2.8 the organisation will submit to audits and inspections, provide the Company with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Company immediately if it is asked to do something infringing data protection law.

Paragraph **13.2**—Contracts with third parties**:**

Recital 81, Articles 28, 29 of Assimilated Regulation (EU) 2016/679, UK GDPR

ICO guide to the UK GDPR: Accountability and governance—Contracts

Whenever a controller uses a processor it needs to have a written contract in place. This paragraph sets out the requirements of that contract, as set out in Article 28(3)

of Assimilated Regulation (EU) 2016/679, UK GDPR. It will obviously be necessary for the employer to ensure that appropriate contracts are in place and that they comply with these requirements. If the employer has any other protections in place in relation to third party processor contracts, they should be reflected in this section of the policy.

13.3 Before any new agreement involving the processing of personal data by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the **[**data protection officer OR [*insert job title or department*]**]**.

Paragraph **13.3**—Consultation with DPO or other responsible person**:**

It will be important to ensure that, before any new contract is entered into that may involve a third party processing personal data, the DPO (or other relevant person or department) has the opportunity to review and approve its provisions to ensure data protection compliance.

Paragraph **13**—Information security**:**

This paragraph anticipates that the organisation may have a separate policy dealing with information policy. See eg Precedent: Policy—information security.

14 Storage and retention of personal data

14.1 Personal data (and special category data) will be kept securely in accordance with the Company's [*information security policy*].

14.2 Personal data (and special category data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained.**[** Staff should follow the Company's [*records retention policy*] which set out the relevant retention period, or the criteria that should be used to determine the retention period.**]** Where there is any uncertainty, staff should consult **[**the data protection officer OR [*insert job title or department*]**]**.

14.3 Personal data (and special category data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Paragraph **14**—Data retention**:**

Article 9(2)(b) of Assimilated Regulation (EU) 2016/679, UK GDPR

DPA 2018, s 10(2), Sch 1 Pt 1, para 1, Sch 1 Pt 4, para 39

Special category data may only be processed for the purpose of performing or exercising rights and obligations under employment law if there is an appropriate policy document in place, ie a policy which:

(a) Article 5 of Assimilated Regulation (EU) 2016/679, UK GDPR

explains the controller's procedures for securing compliance with the principles relating to processing of personal data in connection with the processing of personal data in reliance on the condition in question (see paragraphs 6.7 to 6.9 above), and

(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained

Article 5(1)(e) of Assimilated Regulation (EU) 2016/679, UK GDPR

DPA 2018, Sch 1 Pt 4, paras 39, 40(1)

An appropriate policy document must explain the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition in question, with an indication of how long the personal data is likely to be retained. This Precedent envisages that retention periods, or the criteria used to determine them, will be set out in separate data retention guidelines, as this affords more flexibility to the employer.

For further information, see the sections in Practice Note: The UK GDPR and DPA 2018: lawful processing of personal data in employment: Special category data—specific processing conditions and Appropriate policy document and Precedents: Policy—records retention (employment)and Records retention schedule (employment).

For a sample information policy, see Precedent: Policy—information security.

15 Data breaches

15.1 A data breach may take many different forms, for example:

15.1.1 loss or theft of data or equipment on which personal data is stored;

15.1.2 unauthorised access to or use of personal data either by a member of staff or third party;

15.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

15.1.4 human error, such as accidental deletion or alteration of data;

15.1.5 unforeseen circumstances, such as a fire or flood;

15.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

15.1.7 'blagging' offences, where data is obtained by deceiving the organisation which holds it.

Paragraph **15.1**—Data breaches**:**

Articles 4(12), 33, 34, 83 of Assimilated Regulation (EU) 2016/679, UK GDPR

Given the obligation on organisations to report certain types of data breach to the ICO, and possibly to the individuals affected, it will be important for the policy to identify situations that may give rise to a data breach, so that staff can recognise a breach and report it to the designated DPO (or other responsible person) as required.

15.2 The Company will:

15.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

15.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

Paragraph **15**—Data breaches**:**

Articles 33, 34, 83 of Assimilated Regulation (EU) 2016/679, UK GDPR

A controller is required to report certain types of data breach to the relevant supervisory authority (ie the ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of it. In some cases, the breach will also need to be reported to the individuals affected.

For further information, see Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—Breach notification.

16 International transfers

16.1 **[**The Company will not transfer personal data outside the UK, or to international organisations.

OR

16.2 The Company may transfer personal data outside the UK **[**to [*insert name of country*] **]** and/or to international organisations on the basis **[**that that country, territory or organisation is designated as having an adequate level of protection OR that the organisation receiving the data has provided adequate safeguards by way of **[**binding corporate rules OR standard data protection clauses OR of compliance with an approved code of conduct**]]**.**]**

Paragraph **16**—International transfers**:**

Articles 44–50 of Assimilated Regulation (EU) 2016/679, UK GDPR

UK GDPR imposes restrictions on the transfer of personal data to third countries or international organisations. Personal data may only be transferred outside of the UK or to international organisations in compliance with the conditions for transfer set out in UK GDPR. For further information, see Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—International transfers.

This paragraph provides alternative drafting options depending on whether the employer transfers personal data outside the UK and/or to an international organisation and, if it does, the condition for transfer that applies.

It will obviously be necessary for the employer to ensure that, if required, the appropriate conditions(s) for transfer outside the UK apply.

17 Training

The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Paragraph **17**—Training**:**

Article 24 of Assimilated Regulation (EU) 2016/679, UK GDPR

ICO guide to the UK GDPR: Accountability and governance

A controller must implement appropriate technical and organisational measures that ensure and demonstrate compliance with Assimilated Regulation (EU) 2016/679, UK GDPR. One of the measures suggested by the ICO guidance is staff training.

18 Consequences of failing to comply

18.1 The Company takes compliance with this policy very seriously. Failure to comply with the policy:

18.1.1 puts at risk the individuals whose personal data is being processed; and

18.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Company; and

18.1.3 may, in some circumstances, amount to a criminal offence by the individual.

18.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

18.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact **[**the data protection officer OR [*insert job title or department*]**]**.

Paragraph **18**—Consequences of failing to comply**:**

Articles 58, 83 of Assimilated Regulation (EU) 2016/679, UK GDPR

Given the potentially significant penalties and other enforcement powers of the supervisory authority (ie the ICO), it is advisable to set out for staff the importance of this policy and the consequences of failing to comply with it for them individually (as well as for the employer). For further information, see Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—Enforcement.

I have read and understood this policy and agree to abide by its terms.

Signed.....

This Precedent is an internal-facing data protection policy for use in relation to employees, or other workers and contractors.

Assimilated Regulation (EU) 2016/679, UK General Data Protection Regulation

Data Protection Act 2018

This material considers the UK GDPR regime, and legislative links are to Assimilated Regulation (EU) 2016/679, UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018), except where expressly stated otherwise.

For a client-facing data protection policy (intended for law firms and other professional services providers), see Precedent: Privacy policy—law firms and professional services.

This Precedent takes into account guidance issued by the Information Commissioner's Office (ICO) (see Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—Information Commissioner's Office (ICO) guidance), including:

(a) ICO: Guide to the UK GDPR

the guide to the UK GDPR

(b) ICO: UK GDPR detailed guidance on the right to be informed

detailed guidance on the right to be informed

(c) ICO: UK GDPR detailed guidance on consent

detailed guidance on consent

(d) ICO: Employment information

employment information, including:

(e) ICO: Monitoring workers

monitoring workers

(f) ICO: Information about workers' health

information about workers' health, and

(g) ICO: Information sharing in mental health emergencies at work

information sharing in mental health emergencies at work

Article 29 Working Party: Guidelines on consent under Regulation 2016/679 (wp259rev.01)

It also takes into account the Article 29 Working party (now the European Data Protection Board (EDPB)) guidelines on consent (see Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—Guidelines from the European Data Protection Board (EDPB) (formerly the Article 29 Working Party)).

It identifies, at a high level:

(a) how the employer complies with its obligations under Assimilated Regulation (EU) 2016/679, UK GDPR and DPA 2018, in particular the data protection principles which the employer, as a controller, is required to follow

(b) how staff are expected to handle personal data and sensitive personal data (special category data under UK GDPR and DPA 2018)

(c) the role of the data protection officer (DPO), if there is one (see Practice Note: Data protection officer)

(d) the need for staff to seek further guidance from the DPO or other role holder or department if they have any queries or if they are dealing with complex situations, the scope of which is beyond the remit of this policy, and

(e) the consequences of breach

Article 24 of Assimilated Regulation (EU) 2016/679, UK GDPR

ICO guide to the UK GDPR: Accountability and governance—How can I demonstrate that I comply?

Employers are required to implement appropriate technical and organisational measures that ensure and demonstrate that they process personal data in accordance with Assimilated Regulation (EU) 2016/679, UK GDPR. The ICO guidance on accountability and governance lists a number of measures that an organisation can take. For more detailed information, see Practice Note: The UK GDPR and DPA 2018: key data protection issues for employment lawyers—Accountability.

This Precedent is not a data protection policy of the type that a company would wish to make routinely available to third parties, as it focuses on data protection issues relevant to the processing of staff data, rather than customer or client data.

ICO detailed guidance: The right to be informed

This Precedent is part of a 'layered' approach to drafting (in accordance with the ICO's detailed guidance: The right to be informed), and is intended to be used in conjunction with other relevant policies and privacy notices.

See, for example, Precedents:

(a) Clauses—data protection (employment)

(b) Policy—criminal records information

(c) Policy—data subject access requests

(d) Policy—information security

(e) Policy—bring your own device (BYOD)

(f) Policy—internet, email and communications (or Policy—internet, email and communications (short form))

(g) Policy-social media (or Policy—social media (short form))

(h) Policy—records retention (employment)

(i) Records retention schedule (employment)

(j) Data protection privacy notice (recruitment)

(k) Data protection privacy notice (employment)

(l) Data protection privacy notice (secondment—employer to employee)

(m) Data protection privacy notice (TUPE transfer)

The general detail in Practice Notes: The UK GDPR and DPA 2018: key data protection issues for employment lawyers, The UK GDPR and DPA 2018: lawful processing of personal data in employment and Data protection privacy notices—issues in employment is not replicated in these drafting notes, although numerous references to the relevant sections of the Practice Notes are included throughout. Instead, these drafting notes concentrate on particular drafting issues.

The Lexis®+ UK Employment team recommends that the draft policy should be discussed with employee representatives or a representative sample of employees before it is introduced (see the optional wording in paragraph 2.3).

The Lexis®+ UK Employment team also recommends that the policy should be discussed with new employees as part of their induction process and with existing employees as part of a data protection training programme. The policy should also be made available in the staff handbook and/or on the employer's staff intranet. However, the employer should choose whatever method(s) it considers most effective, in light of the organisation's 'house style' and HR approach.

Article 22 of Assimilated Regulation (EU) 2016/679, UK GDPR

This Precedent assumes that the employer:

(a) ICO guide to the UK GDPR: Children

does not employ children

(b) does not carry out profiling or any other form of automated decision-making

(c) does not record events, movements or driving behaviour in any vehicle the employees drive

(d) does not monitor home or remote working, or employee devices used for work under a Bring Your Own Device (BYOD) policy, or use Mobile Device Management (MDM) services

ICO guide to the UK GDPR: Rights related to automated decision making including profiling

If the employer considers that it has a lawful basis to carry out profiling and/or automated decision-making, ICO guidance recommends that this should be documented in its data protection policy.

For further information on the additional requirements in relation to these types of activity, see Practice Notes: Other data subject rights—issues in employment—Rights related to automated decision-making and profiling and Data processing in the employment relationship [Archived].