

UK GDPR and implementation of diversity issues in a workplace

Chris Burn,
Certified Data Protection Officer,
CSRB Limited





Agenda

PART 1

- ☐ UK GDPR Data Controller Responsibilities
- ☐ UK GDPR Data Processing Principles
- ☐ UK GDPR (Article 6) Lawful Bases for Processing
- ☐ UKGDPR (Article 9) conditions for Processing Special Category Data
- ☐ UK GDPR Rights of Individuals (Data Subjects)

PART 2

- ☐ What is Special Category Data?
- ☐ What is Diversity Data?
- ☐ Setting up a Lawful Diversity Monitoring Process
- ☐ Workplace Accountability Checklist
- ☐ Information Commissioners Office (ICO) Checklist

Chris Burn – Certified Data Protection Officer (DPO) and Managing Director of CSRB Limited

- ❑ Certified Data Protection Officer (C-DPO)
- ❑ Certified Data Privacy practitioner and EU/UK GDPR practitioner
- ❑ Global Association for Software Quality (GASQ) and IT Governance certified
- ❑ CSRB is accredited with the Cyber Essentials certification for cyber and online security assurance
- ❑ International Association of Privacy Professionals (IAPP) speaker
- ❑ Compere, Stand-Up, Comedy & Travel writer
- ❑ Tottenham Hotspur fan (someone has to be!)



A hand-drawn business diagram on a chalkboard. It features a bar chart at the top with an arrow pointing right, a line graph on the right, and a gear at the bottom. A hand is visible on the left side of the chalkboard.

PART ONE – UK GDPR – Data Controller Responsibilities



Data Controller – Article 30 Responsibilities

- ❑ **Information Governance Framework:** you must have a privacy framework of policies, procedures, and scheduled annual UK GDPR training for all colleagues.
- ❑ **Compliance with the Data Processing Principles:** you must comply with the data processing principles listed in [Article 5](#) (Principles relating to processing of personal data) of the UK GDPR.
- ❑ **Individuals' Rights:** you must ensure that individuals can exercise their rights regarding their personal data, including the rights of access, rectification, erasure, restriction, data portability, objection, and those related to automated decision-making.
- ❑ **Accountability Obligations:** you must comply with the UK GDPR accountability obligations, such as maintaining records, and carrying out data protection impact assessments on any Special Category Data processing.
- ❑ **Co-operation with Supervisory Authorities and Professional Codes of Conduct:** you must co-operate with supervisory authorities (such as the ICO) and help them perform their duties, whilst also complying with any industry specific codes of conduct relating to data privacy.
- ❑ **Security:** you must implement appropriate technical and organisational security measures to ensure the security of personal data.



Data Controller – Article 30 Responsibilities

- ❑ **Processor Contracts:** you must enter into a binding contract or other legal act with your Data Processors, which must contain a number of compulsory provisions.
- ❑ **Choosing an Appropriate Processor:** you can only use a Processor that provides sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing meets UK GDPR requirements. This means you are responsible for assessing that your Processor is competent to process the personal data in line with the UK GDPR requirements. This assessment should take into account the nature of the processing and the risks to the Data Subjects.
- ❑ **International Transfers:** you must comply with the UK GDPR's restrictions on transfers of personal data outside of the UK.



Lawful Bases (Article 6)

There are six lawful bases for data processing you can rely on:

1. Consent

2. Contract

3. Legal Obligation

4. Vital Interests

5. Public Task

6. Legitimate Interest

It is the responsibility of the Data Controller to choose which is the most appropriate and document this in all contracts and privacy documentation



Conditions for processing Special Category Data (Article 9)

- (a) Explicit consent
- **(b) Employment, social security and social protection (if authorised by law)**
- (c) Vital interests
- (d) Not-for-profit bodies
- (e) Made public by the data subject
- (f) Legal claims or judicial acts
- (g) Reasons of substantial public interest (with a basis in law)
- **(h) Health or social care (with a basis in law)**
- **(i) Public health (with a basis in law)**
- **(j) Archiving, research and statistics (with a basis in law)**
- If you are relying on conditions (b), (h), (i) or (j), you also need to meet the associated condition in UK law, set out in Part 1 of [Schedule 1 of the DPA 2018](#).



Data Protection Act (2018) – Part One – Conditions relating to Employment or Health

Employment, social security and social protection

This condition is met if:

- (a) the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection
- (b) when the processing is carried out, the controller has an appropriate policy document in place (e.g. appropriate policy document).



Data Protection Act (2018) – Part One – Conditions relating to Employment or Health

Health or social care purposes

This condition is met if the processing is necessary for health or social care purposes. In this description “health or social care purposes” means the purposes of:

- (a) preventive or occupational medicine,
- (b) the assessment of the working capacity of an employee,
- (c) medical diagnosis,
- (d) the provision of health care or treatment,
- (e) the provision of social care, or
- (f) the management of health care systems or services or social care systems or services.



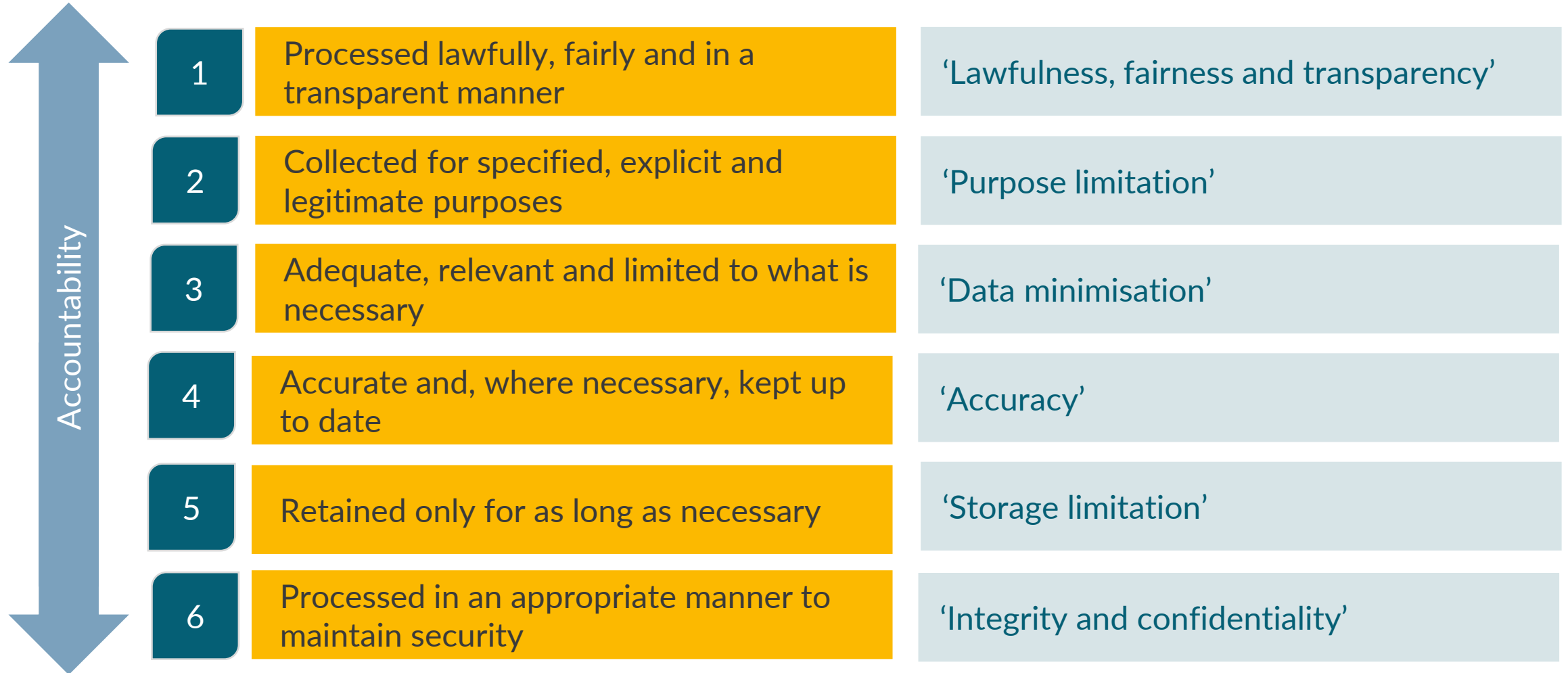
Data Protection Act (2018) – Part One – Conditions relating to Employment or Health

Public health

This condition is met if the processing:

- (a) is necessary for reasons of public interest in the area of public health, and is carried out—
 - (i) by or under the responsibility of a health professional, or
 - (ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

UK GDPR Data Processing Principles



Rights of Individuals (Data Subjects)



A hand-drawn business diagram on a chalkboard. At the top, a bar chart with five bars of increasing height is drawn. Below it, a hand is visible, pointing towards the diagram. To the right of the hand, a large circle is drawn, containing a line graph with several data points. Below the circle, a gear-like shape is drawn. The entire diagram is drawn in white chalk on a dark background. The text "PART TWO – The management of Diversity Data in the Workplace" is overlaid on the diagram in a white box.

PART TWO – The management of Diversity Data in the Workplace



What is Special Category Data?

The UK GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.



What is Diversity Data?

- **Protected characteristics:** Details on race, ethnic origin, religion, sexual orientation, and health.
- **High risk:** This data receives maximum legal protection because its misuse or exposure can lead to discrimination or harm.

Rules for Processing

- **Lawful basis:** Organisations must have a valid lawful basis under the UK GDPR to process any personal data.
- **Extra conditions:** For diversity data, a special category condition is also required.
- **Public interest:** The law allows processing for specific **substantial public interest** reasons, such as monitoring equality of opportunity or treatment at senior levels.
- **Data minimisation:** Organisations should only collect the minimum amount of equality data necessary to achieve their objectives.

Setting up a Lawful Diversity Monitoring Process

1. Conduct a Data Protection Impact Assessment (DPIA)

Before gathering any data, you must complete a DPIA.

- **Identify Risks:** Document why you are collecting this data, how it will be stored, and who will have access to it.
- **Mitigate Exposure:** Establish security protocols to ensure that high-risk sensitive data cannot be linked back to individual employees or job applicants without authorisation.

2. Establish Dual Lawful Bases

You need to identify two separate legal justifications to process this data legally:

- **Core Lawful Basis (Article 6):** Typically, this will be **Legitimate Interests** (to ensure workplace equality)
- **Special Category Condition (Article 9):** Most employers rely on *Schedule 1, Part 2 of the Data Protection Act 2018*—specifically the condition for **Employment, social security and social protection or Statutory/Government purposes** (to identify or maintain equality of opportunity or treatment).

Note on Consent: While explicit consent is an option, the ICO generally discourages relying on consent in an employment context due to the power imbalance between employer and worker.



Setting up a Lawful Diversity Monitoring Process

3. Separate and Anonymise the Data

To respect the principle of data minimisation, your collection process must prevent bias or discrimination:

- **Separate Recruitment Channels:** Ensure diversity monitoring forms are strictly decoupled from the main job application. The hiring panel should never see this sensitive data.
- **Convert to Statistics:** The [ICO's Employment Practices Guidance](#) recommends converting raw diversity data into anonymous, aggregated statistics as quickly as possible. If your organisation is small and anonymity is mathematically difficult, use a fully anonymous survey format instead.

4. Ensure Voluntary and Transparent Collection

Your monitoring forms must be clearly designed to empower the individual:

- **No Compulsion:** Clearly state that filling out the form is completely voluntary and will not impact recruitment or promotion outcomes.
- **The "Prefer Not to Say" Anchor:** Every question (e.g., race, disability, gender identity) must include a "prefer not to say" option.
- **Privacy Notice:** Provide a transparent, easily accessible privacy notice explaining exactly how the data will be used, how long it will be kept, and who handles it.





Workplace Accountability Checklist



Operational Pillar	Direct Mandatory Action	Target Objective
System Ingestion	Ensure every single diversity question contains a "Prefer not to say" anchor option.	Voluntary Transparency
System Ingestion	Ensure an explicit Data Protection Impact Assessment (DPIA) is signed off before deployment.	Risk Mitigation



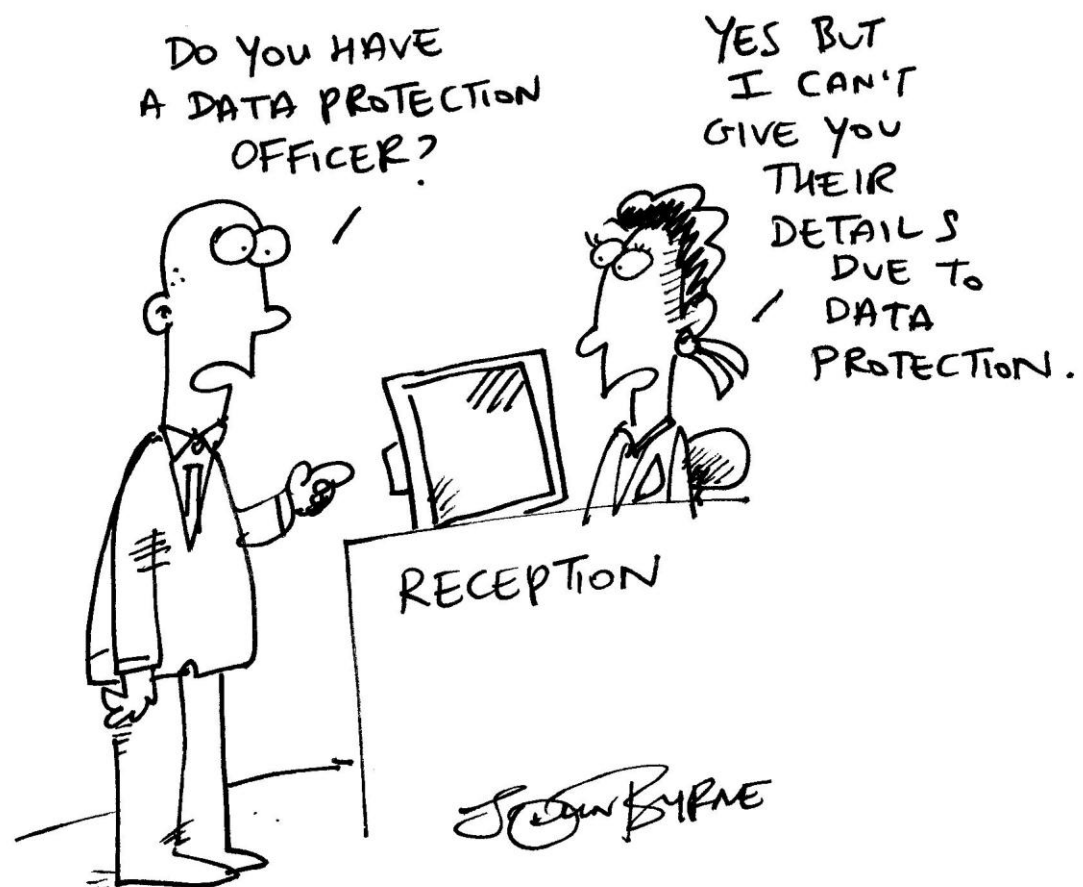
Workplace Accountability Checklist continued.

Operational Pillar	Direct Mandatory Action	Target Objective
Vendor Selection	Verify through service-level agreements (SLAs) that third-party HR platforms are contractually barred from using employee equality metrics to train commercial AI systems.	Purpose Limitation
Lifecycle Deletion	Establish automated deletion scripts to purge or irreversibly aggregate raw survey inputs immediately after high-level statistical summaries are calculated.	Data Minimisation

Information Commissioners Office (ICO) Checklist



- We have checked the processing of the special category data is necessary for the purpose we have identified and are satisfied there is no other reasonable and less intrusive way to achieve that purpose.
- We have identified an UK GDPR Article 6 lawful basis for processing the special category data.
- We have identified an appropriate UK GDPR Article 9 condition for processing the special category data.
- Where required, we have also identified an appropriate DPA 2018 Schedule 1 condition.
- We have documented which special categories of data we are processing.
- Where required, we have an [appropriate policy document](#) in place.
- We have considered whether we need to do a DPIA.
- We include specific information about our processing of special category data in our privacy information for individuals.
- If we use special category data for automated decision making (including profiling), we have checked we comply with UK GDPR Article 22.
- We have considered whether the risks associated with our use of special category data affect our other obligations around data minimisation, security, and appointing Data Protection Officers (DPOs) and representatives.



CartoonStock.com

Questions



Thank You for listening!



Chris Burn

Certified Data Protection Officer and Managing Director at CSRB Limited

E: chris.burn@csrb.co.uk

T: 0117 325 0830

M: 07557 106292



Chris Burn