Data Protection Policy

Introduction and scope

Peritus Health Management provides Customers (Employers) with advice on the management of health risks, the impact on work on health and Data Subjects' (prospective employees or employees) health on their ability to work.

Peritus Health Management places the data security of every Data Subject engaged with its services as a first priority, will ensure that it is transparent in its dealings and processing of data and will remain accountable for its actions and controls.

Peritus Health Management intends to ensure compliance with the requirements of the Data Protection Act 2018 and associated legislation and additional duties of confidentiality that arise from professional guidance and common law in relation to health information.

This Policy sets out the arrangements for Data Protection within Peritus Health Management and should be read in association with:

- Information Governance Policy
- Information Security Policy
- Records Management Policy

Definitions

Definitions associated with Information Governance within Peritus Health Management are included in Appendix 1.

Data Protection Principals

Peritus Health Management recognises and will abide by the 7 key principles of data protection identified by Article 5(1) and Article 5(2) of UK General Data Protection Regulation (ICO, 2018):

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The following arrangements will be implemented to ensure compliance.

Lawful, fair and transparent processing of personal data in relation to individuals.

The lawful basis, purposes, and manner for all service delivery related types of personal data processed within Peritus Health Management are identified in the table in appendix 2.

The lawful basis, purposes, and manner for all business delivery related types of personal data processed within Peritus Health Management are identified in the table in the Information Audit.

All data subjects will be informed about the purposes and manner of personal data processing in a Privacy Notice. The service activities related Privacy Notices will be available on the Peritus Health Management Website (www.peritushealth.com/informationgovernance), in notices within the Peritus Health Management waiting room and mobile screening units, and provided to all data subjects engaged in services provided from the date of implementation of this policy. Due to the complex nature of various categories of data and purposes for processing, Privacy Notices will be specific to the categories of services provided of processing when supplied to individuals so that the information is clear and simple.

The business-related Privacy Notices are available on Sharepoint.

In an exceptional case where Peritus Health Management becomes aware that there is a legal duty to disclose information, for example the data subject constitutes a serious hazard to other workers and/or the general public information may be given to the employer or the relevant authority without consent in the public interest after first discussing the matter with the data subject.

Employees of Peritus Health Management will be provided information, instruction and training on the requirements of legal and professional obligations, business and clinical policies and procedures and will be required to confirm their understanding of their responsibilities before handing data and their competency in all procedures before commencing unsupervised work.

Potential customers requesting information from Peritus Health Management through the website or by telephone enquiry will be required to opt into the storage of their details on the CRM system and advised of this on enquiry.

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Peritus Health Management will ensure that data is not processed for any other purpose than that identified in Appendix 2 or the Information Audit by:

- reviewing the information in appendix 2 and the Information Audit on a regular basis to ensure currency
- ensuring the creation, storage, sharing, transfer, and deletion of data in a secure and efficient manner
- providing training to all staff so that they competently undertake their workplace activities with due regard to the Data Protection Policy and associated policies and procedures
- ensuring that all business and clinical policies and procedures comply with the requirements of the legislation and guidance relating to information governance and are audited on a regular basis by the DPO
- ensuring that the Data Protection Officer or Managing Director is consulted in all change management projects so that data protection is integrated into all processing activities
- not using personal data for marketing purposes without consent
- seeking consent from service users to use their personal details to gain feedback on their experience of the services delivered
- implementing audit processes to confirm adherence to legal and professional obligations, policies, and procedures.

Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed

Peritus Health Management will ensure that the data processed remains limited to what is necessary in relation to the purpose for which they are processed through:

- regular review of business and clinical practices and standardised forms identified in the Document Control Register (PHMF 001.1)
- regular training of staff
- regular audit

Accurate, and where necessary, kept up to date

Peritus Health Management will ensure that the information processed is accurate, and where necessary, kept up to date by:

- identifying the categories of data that should be kept up to date in the table in Appendix 2 and the Information Audit and reviewing the accuracy of the data on a regular basis
- rectifying inaccurate data within 1 month of request, unless there is a substantial reason for not doing so (if patient / client records accurately reflect the author's opinion at the time, based on information given at the time, they may not be inaccurate)
- checking with data subjects during contact, the accuracy of data which is often subject to change (e.g. address, phone number, email address, job titles)
- seeking a regular update of data subject status and data from customers so that data can be archived appropriately
- advising joint data controllers or inaccuracies in data supplied to allow them to amend records
- seeking a list of leavers from Customers on a regular basis
- arranging for the transfer of records to a new provider as appropriate when Peritus Health Management services are no longer required.

Kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed

Peritus Health Management has identified the retention periods for the categories of data processed in Appendix 2 and the Information Audit and has administrative processes in place to ensure that data is archived or erased as appropriate. The latest date for disposal will be used for each data subject's records.

We will ensure that Customers understand their responsibility for the storage of occupational hygiene reports and individual health records (not clinical records) for all their employees exposed to substances and conditions at work that are hazardous to health who are subject to statutory health surveillance.

Where customers are no longer in contact with Peritus Health Management through change of supplier or dissolvement, the date of last entry in the data subjects' records will be used as a reference point for retention periods rather than date of leaving employment.

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

Peritus Health Management has:

- identified suitable and sufficient technical, physical, and organisational measures to ensure the appropriate security of hard (paper) and soft (electronic) data. The security measures are identified in the Information Security Policy.
- processes in place to manage the creation, storage, and retention of records. These processes are identified in the Records Management Policy.

- a process in place for the management of transferring records at the start and end of contracts.

Privacy by design and default

Peritus Health Management has put in place appropriate technical and organisational measures to ensure that the data protection principles are implemented effectively, and individual rights are safeguarded. These include:

- considering data protection issues when planning the implementation of systems, services, and business practices
- assessing risk of data loss or breach and taking steps to prevent harm to individuals and mitigate risk and undertaking a data impact assessment where changes are proposed
- integrating data protection as a priority in all our core functions and ensuring that all employees and subcontractors are provided with appropriate training in data security immediately on commencement and regularly thereafter
- processing only the data we need for the purpose of our activities and only using the data for those purposes
- ensuring IT security to Cyber Essentials standards
- providing easy access to the identity and contact details for the Data Protection Officer within our organisation on our website
- providing Privacy Notices in plain language so that people understand what we are doing with their data
- only using contracted sub-contractors who have provided sufficient guarantees of their ability to ensure data protection by design and take data protection issues into account
- regularly reviewing privacy-enhancing technologies available to assist us in complying with our data protection by design obligations
- undertaking regular audits of data protection requirements and feeding results to Leadership Team to ensure action points are accepted and closed out as appropriate.

Data Subject Rights

Peritus Health Management recognises the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Right to be informed

Peritus Health Management will provide Data Subjects with information on the purposes for processing their personal data, the retention periods for that personal data and who it will be shared with using a combination of different techniques including: an explanation at the start of an appointment, a printed / published Privacy Notice to which the Data Subject is referred.

Right of access

Peritus Health Management will ensure, wherever appropriate, that a data subject has access to all records stored about them. The data subject should apply in writing to Peritus Health Management to request access to the records or for copies of their records to be sent to them.

In order for Peritus Health Management to confirm the identity of the data subject, Peritus Health Management will may request evidence of identity prior to supply. The request for accessing occupational health data (PHMF 010.49) can be used for this purpose.

Peritus Health Management will respond to such a request within 1 calendar month of receipt of the request. Peritus Health Management will provide an individual with an interpretation of information stored in the records where required.

Where a lawyer employed by a company or the data subject requests access to Occupational Health records, Peritus Health Management will ensure that written informed consent has been gained before disclosure. Where there are records related to other matters unrelated to the injury or issue in question, Peritus Health Management will clarify the extent of the consent with the data subject. An Order of Discovery issued by a court or tribunal will be required to gain access to records where consent is refused. The Order of Discovery will be checked for a stamp to clarify that this is a genuine court order.

Where a data subject consents to the release of only part of the Occupational Health records but refuses the release of other equally relevant parts, Peritus Health Management will advise the solicitors of both parties that all the records relevant to the case have not been made available to both sides. Records will not be released in these circumstances without consent or an Order of Discovery.

Right to rectification

If Peritus receives a request to rectification, we will take reasonable steps to satisfy ourselves that the data is accurate (incorrect or misleading as to a matter of fact) and rectify the data if necessary. Peritus will restrict the processing of the Data Subject's data whilst we are considering its accuracy or the legitimate grounds for processing the personal data in question.

If decisions are made on inaccurate data held, the records should confirm both the original inaccurate data, the decisions made, and the accurate data and the date the accurate data was identified.

If the data in question records an opinion, which is in question, the records should show clearly that the information is an opinion and whose opinion it is.

If following investigation Peritus is satisfied that the data is accurate, the Data Subject will be informed that the information will not be amended and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy. A record of the challenge to the accuracy of the data and the reasons for the challenge will be kept with the records.

A request for rectification may also be refused if it is manifestly unfounded or excessive as defined by ICO guidance (ICO, Accessed 25/10/2021).

Right to erasure

The Data Subject has a right to have their personal data erased if:

- if the data is no longer necessary for the purpose for which it was originally collected or processed
- the lawful basis for holding the data was consent and the individual withdraws their consent

- the lawful basis for processing was for legitimate interest, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle)

If the processing of data on the Data Subject is necessary for one of the following reasons the right to erasure does not apply:

- exercise the right of freedom of expression and information
- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for archiving purposes in the public interest, scientific research, historical research, or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing or
- for the establishment, exercise, or defence of legal claims.
- if the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

If Peritus does comply with a request to erase data, they will advise other organisations about the erasure of the data if it has been disclosed to others.

Right to restrict processing

If a Data Subject requests a restriction of processing, this request will be managed by the Managing Director.

Records will be moved into a restricted access filing area labelled 'restriction of processing' until the date of disposal.

Portal records should be marked 'restriction of processing' against the customers name on the portal so that further processing cannot take place.

The further processing of any restricted data other than storage, is prohibited unless:

- we have the individual's consent
- it is for the establishment, exercise or defence of legal claims
- it is for the protection of the rights of another person (natural or legal) or
- it is for reasons of important public interest.

Right to data portability

Data subjects have a right to request their records from Peritus Health Management and supply it to another data controller.

As the data processed by Peritus Health Management is not automated the right to portability does not apply.

Right to object

Any Data Subject who requests that their personal data is not used for direct marketing will be identified on the CRM system and all direct marketing will be stopped immediately.

If a Data Subject objects to the processing of their Data, this should be reported to the DPO or a Director who will review the request in light of the ICO guidance on Right to Object. (ICO, Accessed 25/10/2021)

Roles and Responsibilities

Peritus Health Management is a *Data Controller* for the processing of data in relation to services it provides and the management of the business as it exercises control over what and how data is processed.

The *Managing Director* is responsible for:

- ensuring compliance with legislation and professional guidance
- allocating appropriate resources to fulfil the requirements of the legislation, professional guidance, and this policy
- reviewing this policy on a regular basis to ensure it remains current
- ensuring performance and independence of DPO and responding appropriately to concerns raised.

The *Data Protection Officer* (DPO) is responsible for:

- informing and advising the Directors of Peritus Health Management and its employees about their obligations to comply with the GDPR and other Information Governance legal and professional obligations and ensuring that this Policy is reviewed on a regular basis to ensure currency
- monitoring for changes in legislation and professional guidance in relation to Information Governance, undertake a gap analysis, advise the Managing Director of the changes; creating an action plan to amend business or clinical processes as appropriate in light of any changes, monitoring progress against the action plan and reporting progress to the Managing Director
- to monitor compliance with GDPR and other legal and professional obligations, including business and clinical data processing activities, advising on data protection impact assessments, managing change projects, training staff, and conducting internal audits.
- reviewing the planning for changes in services to ensure GDPR compliance is built into the process
- being the first point of contact for supervisory authorities and for individuals whose data is processed (customers, clients, employees etc)

The *Operations Manager* is responsible for:

- providing all new customers with information on Information Governance and ensuring completion of and compliance with data sharing agreements and ensuring that there is a Data Sharing Agreement in place with all joint controllers before the commencement of data sharing
- feeding audit data into the utilisation report in relation to the maintenance, storage and archiving of customer's client records
- ensuring all marketing activities are compliant
- ensuring data compliance of the Customer Relationship Management system

Departmental leaders are responsible for:

- ensuring all categories of personal data are identified on the Information Audit
- ensuring that the processes implemented within the department comply with the requirements of this policy and are documented in their departmental handbooks
- co-operating with the DPO and auditing processes

- reporting any concerns about the safety, security, and processing of data to the Managing Director and DPO

Employees of Peritus Health Management are responsible for:

- ensuring their compliance with the requirements of this policy and its associated procedures
- ensuring clients (patients) are provided with Privacy Notices appropriate to the services to be supplied and they understand their continued rights for confidentiality within the guiding principles of the Faculty of Occupational Medicine's Ethical Guidance (Faculty of Occupational Medicine, 2012).
- the data they process is accurate, adequate, relevant, and limited to what is necessary
- checking the accuracy of data stored and rectifying inaccurate data as appropriate
- co-operating with the DPO and auditing processes

Customers (employers) are joint controllers with Peritus Health Management as they are responsible for the referral of data subjects to Peritus Health Management and in control of information relating to:

- the data subject
- the data subject's employment status on which Peritus Health Management relies on for the retention and erasure of data
- the hazards to which the data subject is exposed, on which Peritus Health Management relies on for ensuring adequate and relevant data processing and limiting processing of irrelevant data
- the reason for the data subject's referral to or processing by Peritus Health Management

Peritus Health Management and Customers are responsible for ensuring a Data Sharing Agreement is implemented which identifies:

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

Other health care professionals, such as Consultant Specialists, Occupational Physicians, Physiotherapists, Talking Therapists are also joint controllers, as they are responsible for the processing of data in relation to the referrals received from Peritus Health Management.

Peritus Health Management requires a Data Sharing Agreement to be in place to define the responsibilities for data sharing and the practical elements of compliance with all Joint Data Controllers. This Data Sharing Agreement will be reviewed on a regular basis to ensure currency.

Transferring data

Peritus Health Management will only transfer Occupational Health records to an appropriate health professional where the following has been provided:

- confirmation of a contract between the customer and the occupational health provider (a letter from the customer confirming the new provider's details and contact arrangements)
- confirmation from the customer they have consulted with its employees advising of the transfer of services, giving them the opportunity to request for their clinical records to be given to them or their GP rather than transferred, and details of any future storage of records arrangements

- name and GMC / NMC registration number of the person accepting responsibility for the storage and maintenance of the Occupational Health records in accordance with the General Data Protection Regulations (ICO, 2018) and the Faculty of Occupational Medicine's Guidance on Ethics for Occupational Physicians (Faculty of Occupational Medicine, 2012)

A list of all records transferred will be kept and stored.

Electronic records will be transferred on an encrypted memory stick. The stick will be checked by a second person to ensure that the records are encrypted on the stick. The stick will be sent by recorded delivery and the track and trace record will be stored electronically and details of the track and trace provided to the recipient.

The password will be provided to the recipient once they have confirmed receipt of the stick. A copy of the list of all records will be sent to the recipient.

The Occupational Health records are the property of Peritus Health Management and the contents belong to the author.

Where a customer goes into liquidation or refuses to advise Peritus Health Management of the details of the new provider, the records will be retained for the standard periods by Peritus Health Management and where appropriate, copies will be sent to the individual to share with their GP at their own discretion.

Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A data security breach may happen due to:

- loss of theft of data or equipment on which data is stored;
- inappropriate access controls allowing unauthorised use
- equipment failure
- human error
- unforeseen circumstances such as fire or flood
- hacking attack

If a breach has occurred, the employee identifying the breach will immediately advise a Director or DPO who will:

1. take immediate steps to recover the information or confirm deletion
2. establish the likelihood and severity of the resulting risk to people's rights and freedoms and take appropriate steps to reduce / eliminate those risks. The range of adverse effects on individuals, including emotional distress, and physical or material damage, will be considered
3. If the breach is likely to result in a high risk to the rights and freedoms of the data subject, the data subject(s) will be advised of the breach immediately
4. If there is a risk to people's rights and freedoms, the Managing Director or DPO in her absence will report the breach to the Information Commissioners Office and (Customer) no later than 72 hours after the becoming aware of the breach, following current guidance on the ICO website _(ICO, Accessed 2021) .
5. undertake an Incident Corrective Action Report (ICAR) investigation in accordance with the Accident and Incident Corrective Action Reporting Procedure.
6. Report criminal activities
7. Report the findings and action points to the Leadership Meeting

8. Monitoring the action points to ensure completion
9. Review the overall process before closure.

Monitoring Compliance

The DPO will:

- monitor for changes in legislation and professional guidance in relation to Information Governance, and advise the Managing Director of the changes
- work with the Managing Director to create an action plan to amend business or clinical processes as appropriate in light of any changes
- audit against this Policy on a regular basis
- report the outcomes of the audit to the Leadership Meeting

Terms of Reference

European Workplace Drug Testing Society. (2015, Nov 01). *European Guidelines for Workplace Drug Testing in Urine Version 2.0.* Retrieved from European Workplace Drug Testing Society: http://www.ewdts.org/data/uploads/documents/ewdts-urine-guideline-2015-11-01-v2.0.pdf

Faculty of Occupational Medicine. (2012). *Ethics Guidance for Occupational Health Practice.* London: Faculty of of Occupational Medicine.

General Medical Council. (2017, January). *Confidentiality: good practice in handling patient information.* Retrieved from General Medical Council: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality#

ICO. (2011, May). *Data Sharing Code of Practice.* Retrieved from Information Commissioner's Office: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

ICO. (2018, March 22). *Guide to the General Data Protection Regulation (GDPR) 1.0.51.* Retrieved from Information Commissioner's Office: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

ICO. (Accessed 2021 , 10 21). *Report a Breach.* Retrieved from Information Commissioner's Office: https://ico.org.uk/for-organisations/report-a-breach/

ICO. (Accessed 25/10/2021). *Right to Object.* Retrieved from Information Commissioners Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

ICO. (Accessed 25/10/2021). *Right to Rectification.* Retrieved from Information Commissioners Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

Information Commissioner's Office. (2018 Version 1.0). *Data Controllers and Data Processors: what the difference is and what the governance implications are.* ICO. Retrieved from Data Controllers and Data Processors: what the difference is and what the governance implications are.

Information Governance Alliance. (2016, July). *Records Management Code of Practice for Health and Social Care 2016*. Retrieved from Digital NHS: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

Nursing and Midwifery Council. (2015, January 29). *NMC Code.* Retrieved from Nursing and Midwifery Council: https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf

Revision History

Date	Revision No.	Revision description	Revised by	Authorised
25/10/2021	V1	Created as a DPA Policy by reviewing, updating and separating out from Information Governance Policy	OG / AD	AD

Appendix 1 – Definitions

Data - means information which:

Is being processed by means of equipment operating automatically in response to instructions given for that purpose

Is recorded with the intention that it should be processed by means of such equipment

Is recorded as part of a relevant filing system or with the intention that it should forma part of a relevant filing system

Does not fall within paragraph (a), (b), or (c) but forms part of an accessible record as defined by section 68 or

Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

Data Controller – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

Date Impact Assessment -

Data Processor – in relation to personal data, means any person (other than an employee of a data controller) who processes the data on behalf of the data controller

Data Subject – means an individual who is the subject of personal data

Legitimate Interest Assessment – an assessment undertaken to ensure that processing under the lawful basis of 'legitimate interest' is lawful. It is a three-part test that considers: the purpose, necessity and balancing test.

Personal Data – data which relate to a living individual who can be identified –

a) From those data, or
b) From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy Notice - information made available or provided to data subjects when data is processed about them.

Processing – in relation to information or data means obtaining, recording or holding the information or data of carrying out any operation or set of operations on the information or data, including:

a) Organisation, adaptation or alternation of the information or data
b) Retrieval, consultation or use of the information or data
c) Disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) Alignment, combination, blocking, erasure or destruction of the information of data

Recipient – in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure

is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

Relevant filing system – any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, with by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Special Category Data – more Special Category personal data which could create more significant risks to a person's fundamental rights and freedoms e.g. information about an individual's: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics; health; sex life; or sexual orientation

Third party – in relation to personal data, means any person other than –

a) The data subject
b) The data controller, or
c) Any data processor or other person authorised to process data for the data controller or data processor

Appendix 2 – Service Activities Data Process

Service Function	Purpose of Processing	Article 6	Information Processed	Used For	Storage location	Retention Period
Fitness for work	For assessing fitness for work and potential application of the Equality Act	1f - legitimate interests **Article 9** 2f & h – the establishment, exercise or defence of legal claims & preventive / occupational medicine	Name, Date of Birth, Address, Job Title and description of duties, Telephone number, GP surgery, Physical and mental health diagnoses Family and social history and arrangements Wellbeing issues Employment issues which may impact on health, Sickness Absence History, Outstanding Management Issues; Adjustments / Restrictions to duties implemented; Action Pertinent details of discussion; Risk assessments. Medical history, functional capacity, opinion of fitness for work, adjustments, recommendations or restrictions suggested, information relating to opinion on health risks and health risk management and employment, opinion on disability status	Identification of employee, records maintenance, invoicing, quality management, assessing health status and work capacity in relation to job requirements and establishing fitness for work, restrictions and adjustments duty are required or recommended in order to protect the employee and allow them to achieve their optimum potential. Updating / arranging further medical / healthcare support	Portal **3rd Party Sharing Route** Customer through Portal Client through Portal or Recorded Post Contracted OH Physician or Clinician through Portal Specialist Healthcare Provider (if referred) encrypted email	6 years after leaving or date of last entry
Health Surveillance	To undertake statutory health surveillance programmes of employees on behalf of the customer to aid the employee with early detection and management of disease	**Article 6** 1f - legitimate interests **Article 9** 2f & h – the establishment, exercise or defence of legal claims & preventive / occupational medicine	Name, Date of Birth, Address, Job Title and description of duties, Telephone number, GP surgery, Family and social history and arrangements Wellbeing issues Medical history, exposure history, occupational history, physical measurements, examination history Opinion on outcome and fitness for work	Identification of employee, records maintenance, invoicing, quality management, early detection of disease; assessment of fitness for work; and review of suitability and sufficiency of health and safety control measures. Updating / arranging further medical / healthcare support	**Storage location** Portal **3rd Party Sharing Route** Customer through Portal Client through Portal or Recorded Post Contracted OH Physician or Clinician through Portal Specialist Healthcare Provider (if referred) encrypted email	10 years after leaving or date of last entry

Service Function	Purpose of Processing	Article 6	Information Processed	Used For	Storage Location	Retention Period
Talking Therapies	To fulfil professional responsibilities for record keeping and referrals to specialist healthcare if required.	1b – contract 1c – legal obligation 1d – Vital interests 1f - legitimate interests **Article 9** 2f & h – the establishment, exercise or defence of legal claims & preventive / occupational medicine	Name, Date of Birth, Address, Telephone number, email address, GP surgery, Physical and mental health diagnoses Family and social history and arrangements Wellbeing issues	Identification of employee, records maintenance, invoicing, quality management, Updating / arranging further medical / healthcare support	Limited access Sharepoint **3rd Party Sharing Route** Specialist Healthcare Provider (if required) Emergency services if required	6 years after date of last entry
Biological Monitoring	To establish whether there are any biological indicators of exposure so that the customer can review the suitability and sufficiency of their health and safety control measures.	**Article 6** 1f - legitimate interests **Article 9** 2f & h – the establishment, exercise or defence of legal claims & preventive / occupational medicine	Name, Date of Birth, Address, Job Title and description of duties, Telephone number, Physiological results	Identification of employee, records maintenance, invoicing, quality management, early detection of disease; assessment of fitness for work; and review of suitability and sufficiency of health and safety control measures. Supporting information, instruction and training programmes for employees	**Storage location** Portal **3rd Party Sharing Route** Customer through Portal Client through Portal or Recorded Post Contracted OH Physician or Clinician through Portal Specialist Healthcare Provider (if referred) encrypted email	10 years after leaving or date of last entry

Service Function	Purpose of Processing	Article 6	Information Processed	Used For	Storage Location	Retention Period
Pregnancy / Health Risk Assessment	To establish whether there is a risk to health from workplace activities and determine what control measures are required to manage risk	1f - legitimate interests **Article 9** 2f & h – the establishment, exercise or defence of legal claims & preventive / occupational medicine	Name, Date of Birth, Address, Job Title and description of duties, Telephone number, GP surgery, Family and social history and arrangements Wellbeing issues Medical history, exposure history, occupational history, physical measurements, examination history Photos of work activities Exposure monitoring results Opinion on outcome and fitness for work	Identification of employees, records maintenance, invoicing, quality management, and provide a report on health and safety risk and control measures	Portal **3rd Party Sharing Route** Customer through portal / email / post	10 years after leaving or date of last entry
Occupational Hygiene	To establish whether there are any indicators of exposure so that the customer can review the suitability and sufficiency of their health and safety control measures	**Article 6** 1f - legitimate interests **Article 9** N/A	Name, Date of Birth, Address, Job Title and description of duties, Telephone number, Photos of work activities Exposure monitoring results	Identification of employees, records maintenance, invoicing, quality management, and review of suitability and sufficiency of health and safety control measures Supporting information, instruction and training programmes for employees	**Storage Location** Portal **3rd Party Sharing Route** Customer through portal / email / post	10 years after leaving or date of last entry
Drugs and Alcohol Testing	To establish whether there are measurable indications of drugs and alcohol use	**Article 6** 1f - legitimate interests **Article 9** 2f & h – the establishment, exercise or defence of legal claims & preventive / occupational medicine	Name, Date of Birth, Address, Job Title and description of duties, Telephone number, Physiological results	Identification of employee, records maintenance, invoicing, quality management, and reporting on outcome as per purpose.	**Storage Location** Portal **3rd Party Sharing Route** Customer through portal / email / post	6 years after leaving or date of last entry

Service Function	Purpose of Processing	Article 6	Information Processed	Used For	Storage Location	Retention Period
Ill Health Retirement	To establish an employee's work capacity in relation to Pension Fund Ill Health Retirement Criteria	1f - legitimate interests **Article 9** 2f & h – the establishment, exercise or defence of legal claims & preventive / occupational medicine	Name, Date of Birth, Address, Job Title and description of duties, Telephone number, National Insurance Number, Employment issues which may impact on health, Sickness Absence History, Outstanding Management Issues; Adjustments / Restrictions to duties implemented; Action Taken by Management; Pertinent details of discussion; Risk assessments. Leaving Date, Pension Fund details Medical history, functional capacity, opinion of fitness for work, adjustments, recommendations or restrictions suggested, information relating to opinion on health risks and health risk management and employment, opinion on disability status, ill health retirement forms	Identification of employee, records maintenance, invoicing, quality management, assessing health status and work capacity in relation to job requirements; establishing fitness for work in relation to the Pension Fund's criteria for early retirement on the grounds of ill health; supporting application for early retirement on the grounds of ill health. Updating / arranging further medical / healthcare support	Portal **3rd Party Sharing Route** Customer through Portal Client through Portal or Recorded Post Contracted OH Physician or Clinician through Portal Specialist Healthcare Provider through recorded post	6 years after leaving or date of last entry
Face Fit Testing	to establish whether there are qualitative indications that the respiratory protective equipment issued to employees is suitable and sufficient and fulfils the customer's duty of care to the employees	**Article 6** 1f - legitimate interests **Article 9** N/A	Name, Date of Birth, Address, Job Title and description of duties, Telephone number, Mask types, facial features Test results	Identification of employee, records maintenance, invoicing, quality management, and confirming suitability and sufficient of the respiratory protective equipment.	**Storage Location** Portal **3rd Party Sharing Route** Customer through Portal	6 years after leaving or date of last entry

Service Function	Purpose of Processing	Article 6	Information Processed	Used For	Storage Location	Retention Period
Aural Impressions	To create moulding for production of personal hearing protection	1b – contract Article 9 N/A	Name, Date of Birth, Address, Job Title Telephone number, aural impression	Identification of employee, records maintenance, invoicing, quality management	Portal 3rd Party Sharing Route Customer through Portal	6 years after leaving or date of last entry