Aberdeen Orthopaedic Network

Policy for General Data Protection Regulations (GDPR) Compliance

Version 1.1 March 2018

Data Protection Compliance Manager:

[name/email] (2018)

Contents

Introduction

- The General Data Protection Regulation (GDPR) has effect in the UK from **25 May 2018**.
- It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection regarding how their personal data is used by organisations.
- Aberdeen Orthopaedic Network (hereafter 'AON') must comply with its requirements, just like any other charity or organisation.
- There are very significant fines (up to €20 Million) for non-compliance.
- AON must provide evidence of its compliance under the 'principle of accountability' – we cannot just say we are compliant.
- AON must honour the subject's rights (set out in Appendix 2)

Underlying Principles

The GDPR has a number of underlying principles with which we must comply. These include that personal data:

- Must be **processed** lawfully, fairly and **transparently.**
- Is only used for a **specific processing purpose** that the data subject has been made aware of and no other, without further consent.
- Should be "**adequate, relevant and limited**." i.e. only the minimum amount of data should be kept for specific processing.
- Must be "**accurate** and where necessary **kept up to date**".
- Should not be stored for longer than is necessary, and that **storage is safe** and secure.
- Should be processed in a manner that ensures appropriate **security and protection.**

This suite of policies and procedures has two important functions – it offers assurance to the subjects about whom we hold data, and it also offers assurance to us as an LLP that we are behaving appropriately and have the right procedures in place to protect people's information and only use it in accordance with their wishes.

There are several sub sections to this document:

SECTION 1: Data protection policy
This is a policy which sets out the standards that AON expect to be adhered to by anyone who is dealing with personal information on behalf of the LLP.

Circulation: all staff and groups who hold personal information.

SECTION 2: Retention of Records policy
Data should only be kept as long as is necessary. This policy sets out how long different types of data will be kept, how it will be shared and how it should be deleted.

SECTION 3: Information security policy
This is the policy which sets out the way the LLP will ensure preservation of confidentiality, prevention of unauthorised access, maintaining of integrity and safeguarding of accuracy of information within the LLP data.

SECTION 4: Consent & Privacy Notices
These are the essential documents that must be used to inform and record consent for those whom we hold data on ('subjects').

SECTION 5: Data Breach policy
If our systems fail to prevent a data breach, we have obligations under GDPR to inform and then to review our systems to reduce risk of further breaches.

SECTION 1:

Data protection policy

This is our policy which sets out the standards that AON expect to be adhered to by anyone who is dealing with personal information on behalf of the LLP.

Anyone who uses or processes any personal information on behalf of the LLP must be familiar with and follow the processes laid out in this policy.

"Data Protection Legislation"…	means the Data Protection Act 1998, the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, including, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office.

Data Protection Legislation ("the Legislation") is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully and that where necessary the privacy of individuals is respected. During the course of the activities of AON, the LLP will collect, store and process personal data about our members, people who seek our services and activities, suppliers and other third parties and we recognise that the correct and lawful treatment of this data will maintain confidence in the LLP. This policy sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

The **Data Protection Compliance Manager** is responsible for ensuring compliance with the Legislation and with this policy.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

Processing personal data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy carries potentially serious consequences and may result in disciplinary action.

'Processing' includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.

Personal data is data relating to a living individual. It includes employee data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered.

Important:
Personal data can be factual (for example a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Examples of personal data are employee details, including employment records, names and addresses and other information relating to individuals, including supplier details, any third party data and any recorded information including any recorded telephone conversations, emails or CCTV images.

Employees and others who process data on behalf of the LLP should assume that whatever they do with personal data will be considered to constitute processing.

Individuals should only process data:

- If they have consent to do so; or
- If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll

If neither of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

Measures for specific aspects of data handled by AON are detailed below.

The following general provisions shall be applied in all cases:

1. Data will only be stored physically in the LLP offices in a locked cabinet or safe or electronically on a computer owned by the LLP.
2. All computers owned by the LLP shall require to have industry standard virus protection software in line with IT advice received and this shall be updated regularly.
3. All computers owned by the LLP shall be required to have password protection in place
4. It shall not be acceptable for data to be transferred to any third party or personal data storage equipment by any employee or agent of the LLP without explicit

permission from the subjects concerned so to do. Any breach of this aspect of policy will require reporting as a data breach and shall be considered under the LLP serious misconduct policy for employees.

5. All those who process data for AON shall be required to familiarise themselves with this policy and confirm their awareness and understanding of its contents. They will be required to attend training when organised.

Compliance with the Legislation

Employees and others who process data on our behalf have a responsibility for processing personal data in accordance with the Legislation. Anyone who has responsibility for processing personal data must ensure that they comply with the data protection principles in the Legislation. These state that personal data must:

- be obtained and used fairly and lawfully
- be obtained for specified lawful purposes and used only for those purposes
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for any longer than required for those purposes
- be used in a way which complies with the individual's rights (this includes rights to prevent the use of personal data which will cause them damage or distress, to prevent use of personal data for direct marketing, and to have inaccurate information deleted or corrected)
- be protected by appropriate technical or organisational measures against unauthorised access, processing or accidental loss or destruction
- not be transferred outside the European Economic Area unless with the consent of the data subject or where the country is determined to have adequate systems in place to protect personal data.

Monitoring the use of personal data

We are committed to ensuring that this data protection policy is put into practice and that appropriate working practices are being followed. To this end the following steps will be taken:

- any employees who deal with personal data are expected to be aware of data protection issues and to work towards continuous improvement of the proper processing of personal data;
- employees who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored;
- All employees must evaluate whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure inaccurate, excessive or out of date data is disposed of in accordance with this policy;
- Spot checks may be carried out;
- An annual report on the level of compliance with or variance from good data protection practices will be produced by the Data Protection Compliance Manager.

- Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

To facilitate compliance we will undertake a Data Audit:

Data Audit

All individuals who hold or use any personal data on behalf of AON are required to declare that to the Data Protection Compliance Manager by completing a Data audit form (see Appendix 3).

The data audit will be used by the Data Protection Compliance Manager to consider and recommend improvements to our data protection measures and introduce mitigations for potential data breach risks.

The responsibility for the approval and enforcement and review of this policy rests collectively with the Board of Directors of AON LLP.

The Data Protection Compliance Manager shall lead a review of this policy on an annual basis and report to the Board.

Any new process or technology introduced that may have any bearing on personal data shall be subject to a **Data Protection Impact Assessment** before its introduction. The Data Protection Compliance Manager must be satisfied that sufficient safeguards have been built in to any new system to at least match preexisting levels of security.

Handling personal data and data security

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. Manual records relating to individuals or staff will be kept secure in locked cabinets. Access to such records will be restricted. Computer files should always be password protected.

We will ensure that staff and members who handle personal data are adequately trained and monitored.

We will ensure that passwords and physical security measures are in place to guard against unauthorised disclosure.

We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out below).

Security policies and procedures will be regularly monitored and reviewed to ensure data is being kept secure.

Where personal data needs to be deleted or destroyed adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files. Particular care will be taken

over the destruction of manual sensitive data (written records) including shredding or disposing via specialist contractors.

All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed. Any agent employed to process data on our behalf will be bound to comply with this data protection policy by a written contract. Personal data stored on a laptop must be password protected.

The rights of individuals

The Legislation gives individuals certain rights to know what data is held about them and what it is used for. In principle everyone has the right to see copies of all personal data held about them. There is also a right to have any inaccuracies in data corrected or erased. Data subjects also have the right to prevent the processing of their data for direct marketing purposes.

Any request for access to data under the Legislation should be made to the 'GDPR Manager of AON LLP' in writing. In accordance with the Legislation we will ensure that written requests for access to personal data are complied with within 30 days of receipt of a valid request.

When a written data subject access request is received the data subject will be given a description of
a) the personal data,
b) the purposes for which it is being processed,
c) those people and organisations to whom the data may be disclosed,
and be provided with a copy of the information in an intelligible form.

The six lawful bases for data processing

In order to process data AON recognizes that it must identify in its privacy notices which lawful basis/bases we are processing that data.

1. Consent
For those <u>not holding a role</u> within the LLP, this will be the most common reason. We must demonstrate we have obtained consent:
Transparently – The purpose was clear
Explicitly – The consent is written
Specific – We set out clearly the extent of and purposes of collecting the data
Unambiguous – The consent is clearly and positively given, not implied

2. Legitimate interests

This involves a balancing test between the LLP's legitimate interests and the interests or fundamental rights of and freedoms of the data subject – in particular where the data subject is a child. The privacy policy of a controller must inform data subjects about the legitimate interests that are the basis for the balancing of interests.

The Balancing Test:

a) Identify the LLP's legitimate interest - What is the purpose of the processing and why is it important?

b) Carry out a 'necessity test' - Is there another way of achieving your legitimate interest? If the answer is no, then it is necessary.

c) Carry out a 'balancing test'

- Does the data subject's right override the legitimate interest?
- Consider the nature of the processing, its impact and what mitigation you can put in place.
- What possible negative impacts for privacy could there be.

The outcome must be recorded and stored by the GDPR Data Manager.

3. Contractual necessity

Personal data may be processed if the processing is necessary in order to enter into or perform a contract with the data subject (or to take steps prior to entering into a contract).

4. Compliance with legal obligation

Personal data may be processed if the processing is necessary to fulfill a legal requirement. Records to comply with Safeguarding are permissible under this category.

5. Vital interests

In life or death situations, personal data may be used without consent – eg to contact a relative in an emergency.

6. Public interest

Public authorities may invoke this reason. It is unlikely to be applicable in the LLP situation.

'Special category data' - Sensitive personal data rules

We will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards can be put in place. Sensitive data means data consisting of information relating to an individual's

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal offences

Sickness records are likely to include sensitive data and as such should only be held if the explicit consent of each employee is obtained or if one of the other conditions for processing sensitive data is satisfied.

In order to process this data AON recognizes the need to

a) Establish a lawful basis/bases and

b) Establish at least one of the following:

Explicit consent of the data subject has been obtained (which can be withdrawn).

Employment Law – if necessary for employment law or social security or social protection.

Vital Interests – e.g. in a life or death situation where the data subject is incapable of giving consent.

Charities, religious organisations and not for profit organisations – to further the interests of the organisation on behalf of members, former members or persons with whom it has regular contact such as donors. Note, however, that explicit consent is required for the personal data to be shared with a third party.

Data made public by the data subject – the data must have been made public 'manifestly'.

Legal claims – where necessary for the establishment, exercise or defence of legal claims or for the courts acting in this judicial capacity.

Reasons of substantial public interest – where proportionate to the aim pursued and the rights of individuals are protected.

Medical Diagnosis or treatment – where necessary for medical treatment by health professionals including assessing work capacity or the management of health or social care systems.

Public Health – where necessary for reasons of public health e.g. safety of medical products.

Historical, Statistical or scientific purposes – where necessary for statistical purposes in the public interest for historical, scientific research or statistical purposes.

Delegated roles

a) Financial Records

1. All individuals with data in AON financial records will require to have consent in place, including:
    a. Donors
    b. Employees
    c. Creditors (those whom we employ on an ad hoc basis eg for repairs)
    d. Debtors (those who may owe the Trust money for a service rendered, eg course fees).
2. The detail of AON finances will be reserved to the Bookkeeper, the Treasurer, our Bankers and our authorized Accountants.
3. It shall be confirmed by the Treasurer that GDPR provisions at the Bank and at the Accountants are appropriate.
4. Data stored for employees, creditors, donors and debtors shall be limited to
    a. Name of account holder
    b. Address of account holder
    c. Account number, sort code, Bank name and address
    d. Amounts paid in/out and frequency/term thereof
    e. Any additional information will be stipulated to the individual and consent sought
5. All financial data (statements from bank, letters etc) shall be stored in a locked cabinet in the office or, where electronically stored, on an LLP-owned computer which shall have in place industry standard firewall/virus protection and password access.

6. The sharing of data from the financial records of the LLP shall only be to HMRC to comply with their lawful requirements.

c) Employee Records

1. All prospective employees must return a signed consent form and receive a General Privacy Notice at the time they apply as a condition of application.
2. Any updates to the employee records shall be the responsibility of the Delegated officer of the LLP stipulated above, with the official record being held by the Secretary of the LLP.

d) General IT and AV

1. Any images or data captured in any format within the LLP shall be subject to data protection regulations. These include but are not limited to:
    a. Photographic records and Video footage of events
    b. Electronic communications
    c. Broadcast information (on the web or in another format)
    d. The website
    e. Any projected content
    f. Images reproduced in any format on behalf of the LLP
2. Where the LLP operates any CCTV equipment it will display prominent notices in the area under surveillance.
3. The LLP shall actively seek permission from anyone included in image capture of any kind and undertakes to avoid capture of but further to protect images of those who do not grant such permission from accidental use.
4. On any occasion that images are to be captured on behalf of the LLP which include any personally identifiable data (including a photo of written information or a person's image) the person capturing those image(s) must seek advice in advance from the delegated responsible person (see above) regarding consent.
5. The data protection compliance manager will be able to offer further support.
6. See the Information Security Policy for more information.

Changes to this policy

We reserve the right to change this policy at any time. Where appropriate we will notify data subjects of those changes by mail or email.

Policy adopted on ……..

Review due……

SECTION 2:

Retention Policy

Storage of Data and Records Statement

1. All data and records will be stored in accordance with the security requirements of the Data Protection Legislation and in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

2. Data and records which are active should be stored in the most appropriate place for their purpose commensurate with security requirements.

3. Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose.

4. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.

5. Any data file or record which contains personal data of any form can be considered as confidential in nature.

6. Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Legislation, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose". All groups are required to have regard to the Guidelines for Retention of Personal Data attached hereto.

7. Any data that is to be disposed must be safely disposed of for example by shredding. Any group which does not have access to a shredder should pass material to the LLP secretary who will undertake secure shredding.

8. Special care must be given to disposing of data stored in electronic media. Guidance will be given by the Data protection manager to anyone who has stored data on for example personal computers which are to be disposed of.

Policy adopted on ……..

Review due……

Guidelines for Retention of Personal Data

(This is not an exhaustive list)

If you have any queries regarding retaining or disposing of data please contact the Data Protection Compliance Manager.

Each delegated responsible person shall review the records for which they are responsible and undertake an appropriate cull of data no longer required on an at least annual basis.

Types of Data	**Suggested Retention Period**
Personnel files including training records and notes of disciplinary and grievance hearings.	• 6 years from the end of employment
Application forms / interview notes	• Maximum of one year from the date of the interviews for those not subsequently employed. If employed, retain in personnel file.
Information relating to children	• Check for accuracy once a year • Record that child was a member of the group – permanent • Secure destruction of personal data other than name and fact of membership – three years after cease to be a member
Database / contact information	• Check for accuracy once a year • Secure destruction of personal data other than name and fact of contact – three years after cease to be active contact
Income Tax and NI returns, including correspondance with tax office	• At least 6 years after the end of the financial year to which the records relate
Statutory Maternity Pay records and calculations	• As Above • (Statutory Maternity Pay (General) Regulations 1986)
Statutory Sick Pay records and calculations	• As Above • Statutory Sick Pay (General) Regulations 1982
Wages and salary records	• 6 years from the tax year in which generated
Accident books, and records and reports of accidents	• (for Adults) 3 years after the date of the last entry • (for children) three years after the child attains 18 years (RIDDOR 1985)

Health records	• 6 months from date of leaving employment • (Management of Health and Safety at Work Regulations)
Health records where reason for termination of employment is connected with health, including stress related illness	• 3 years from date of leaving employment • (Limitation period for personal injury) claims)
Student records, including academic achievements, and conduct	• At least 6 years from the date the student leaves in case of litigation for negligence

SECTION 3:

Information security policy

Information security involves preserving confidentiality, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users.

In addition to complying with this policy, all users must comply with the Data Protection Legislation and the Data Protection Policy.

'AON data' means any personal data processed by or on behalf of the LLP.

*Information security is the responsibility of **every** member of staff, Partner using data on but not limited to AON information systems.*

Our IT systems may only be used for authorised purposes. We will monitor the use of our systems from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

We will ensure information security by:

a) Ensuring appropriate software security measures are implemented and kept up to date;
b) Making sure that only those who need access have that access;
c) Not storing information where it can be accidentally exposed or lost;
d) Making sure that if information has to be transported it is done so safely using encrypted devices or services.

Access to systems on which information is stored must be password protected. Passwords must not be disclosed to others. If you have a suspicion that your password has been compromised you must change it.

You must ensure that any personally owned equipment which has been used to store or process AON data is disposed of securely. Software on personally owned devices must be kept up to date.

Do not use unsecured wifi to process AON data.
All breaches of this policy must be reported to the Data Protection Compliance Manager.
This policy will be regularly reviewed and audited.

The following information shall be used alongside any professional guidance deemed necessary :

https://www.jisc.ac.uk/guides/security-mobile-devices-and-data-protection

Policy adopted on ……..

Review due……

SECTION 4:

Consent & Privacy Notices

Under GDPR the AON LLP is required to obtain and retain explicit written consent for each individual about whom we store and process data.

A consent form is located in Appendix 4. Each individual will be supplied with a 'General Privacy Notice' (see appendix 5) which will also be made available on the LLP website.

Children under 13 about whom data is processed will require consent from someone with parental responsibility. Our paperwork will be in language that is understandable.

Those with specified roles in the LLP are unable to give or withdraw their consent 'freely' (since their role is dependent on implicit ongoing consent) and are therefore to receive a 'Specified Role Privacy Notice' (see appendix 6).

The LLP note that an opt in consent is required for most communications with individuals.

The following roles are specified within AON:

1. All Partners
2. All Employees

SECTION 5:

Data breach policy

AON takes every care to protect the data we hold. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties.

A data breach is defined as an accidental or unlawful destruction/loss/alteration/unauthorized disclosure of or access to personal date.

This policy sets out the procedure to be followed to ensure a consistent and effective approach throughout the LLP to minimize risk and respond appropriately to a breach.

The policy relates to all personal data held by AON LLP, regardless of format. It applies to anyone who handles this personal data, including those working on behalf of the LLP. The objective of the policy is to contain any breaches, to minimise the risks associated with the breach and to consider what action is necessary to secure personal data and prevent any further breach.

Types of breach
An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects.
An incident includes but is not restricted to:

- Loss or theft of personal data or the equipment on which the data is stored e.g. laptop, memory stick, smartphone, or paper record
- theft or failure of equipment on which personal data is stored
- Unauthorised use of or access to personal data
- Attempts to gain unauthorised access to personal data
- Unauthorised disclosure of personal data
- Website defacement
- Hacking attack

Reporting an incident
Any person using personal data on behalf of AON LLP is responsible for reporting data breach incidents immediately to the Data Protection Compliance Manager or in his or her absence the Secretary of the LLP. The report should contain the following details:

- Date and time of discovery of breach
- Details of person who discovered the breach
- The nature of the personal data involved
- How many individuals' data is affected

Containment and recovery

The Data Protection Containment Manager/LLP Secretary will act as the **Investigating Officer (IO)** for the LLP.
The IO will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required.
Consideration will be given as to whether the police should be informed.
Advice from appropriate experts will be sought if necessary.
A suitable course of action will be taken to ensure a resolution to the breach.

Investigation and risk assessment
An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. The IO will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to occur.

The investigation will take into account the following:

- The type of data involved and its sensitivity
- The protections in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to illegal or inappropriate use
- Who the data subjects are, how many are involved, and the potential effects on them
- Any wider consequences

Notification
The IO will decide with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case by case basis. Consideration will be given to notifying the Information Commissioner if a large number of people are affected or the consequences for the data subjects are very serious. Guidance on when and how to notify the ICO on their website www.ico.org.uk/media/1536/breach_reporting.pdf will be consulted.
The Trust recognizes its duty to record and report any serious data breach to the ICO within 72 hours of finding out about it. This responsibility is delegated to the GDPR Responsible Officer. In their absence an office bearer of the LLP (Secretary or Treasurer) will be responsible for the notification.
Notification to the data subjects whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the nature of the data involved. Specific and clear advice will be given on what they can do to protect themselves and what has already been done to mitigate the risks.
The IO will keep a record of all actions taken in respect of the breach – see Appendix 8.

Evaluation and response
Once the incident is contained, The IO will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring.

The nature of the breach, any mitigations that can be put in place to limit its impact and actions to address any resultant problems will be recorded and conveyed to the ICO.

Training

The LLP shall organize a meeting at least annually for those with specified roles to meet and discuss the policy.
All those with specified roles shall be required to sign to confirm they have received and understand a copy of this policy (see appendix 7).

Funded training opportunities will be considered by the LLP.

Concerns Process
The AON LLP ("we") take your privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact The Secretary of the LLP without delay.

We will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation. We will keep you informed of the progress of our investigation and the outcome. If you are not satisfied with the outcome, you may wish to contact the Information Commissioner's Office at https://ico.org.uk/concerns/
Any complaint received by us must be referred to the Secretary of the AON LLP who will arrange for an investigation as follows:

1. A record will be made of the details of the complaint.
2. Consideration will be given as to whether the circumstances amount to a breach of Data Protection Legislation and action taken in accordance with the Data Breach Procedure.
3. The complainant will be kept informed of the progress of the complaint and of the outcome of the investigation.
4. At the conclusion of the investigation the Data Protection Compliance Manager will reflect on the circumstances and recommend any improvements to systems or procedures.

APPENDIX 1: Glossary of terms

Personal data is information about a living individual from which it is possible to identify that individual. E.g. names, email addresses, photos.

Sensitive personal data (which has a higher threshold of protection) includes genetic data, biometric data and data concerning sexual orientation, in addition to categories such as religious belief, race/ethnic origin, trade union membership, health and criminal records.

Processing is anything done with/to personal data, including storing it.

The ***data subject*** is the person about whom personal data is processed.

The ***data controller*** is the person or organisation who determines the how and what of data processing, in this case it is the LLP.

The ***organization*** is the legal entity relevant to this legislation which is the LLP, is intrinsically required to comply with this policy since it acts within and on behalf of the legal entity which is the LLP.

The ***GDPR Responsible Manager*** is the individual agreed by the Board to take the lead role in the implementation of this policy, to report on compliance to the Board and to raise any issues or concerns to the officers of the Board (The Chair or Secretary) immediately they become apparent.

APPENDIX 2: Subject rights

GDPR sets out the following rights that the LLP must honour:

1. The right to be informed

Individuals continue to have a right to be given "fair processing information", usually through a 'privacy notice'. Under the GDPR there is additional information that we will need to supply. For example, we must explain the lawful basis for the processing of their data; our data retention periods (how long we keep it for) and that individuals have a right to complain to the ICO if they think that there is a problem in the way that we deal with their personal data.

2. The right to access (includes subject access requests)

Under the GDPR the right of data subjects to request information about the personal data processed by organisations requires a response without undue delay and in any case within one month of receipt of the request. No fee is chargeable.

We are able to refuse or charge a "reasonable fee" for requests that are manifestly unfounded, excessive or repetitive. If we do refuse a request you must tell the individual why and that he/she has the right to complain to the ICO or go to court.

3. The right to rectification (correction)

Individuals have the right to have their personal data corrected (rectified) if it is inaccurate or incomplete. If the data has already been given to third parties, the Trust must tell those third parties of the correction. We must also tell the individuals about the third parties to whom the data has been given.

4. The right to erasure (also known as the right to be forgotten)

Data subjects have the right to request the removal or erasure of their personal data, for example if it is no longer necessary to process their data, the individual objects to such processing and/or the individual withdraws consent. Not only will we need to comply with such requests but we will also need to ensure that any third party with whom the data was shared also deletes such data.

This does not mean that a person can immediately request that his/her personal data is deleted. If the purposes for which the data was collected still exist, then a person will not be able to request the deletion of that data, unless it was given by consent and they are

withdrawing their consent. This is one reason why consent is not the appropriate lawful basis for data processed in connection with a person's role in the LLP. For instance, safeguarding information about an individual cannot be deleted if the retention is still necessary, reasonable and proportionate - e.g. to protect members of the public from significant harm. Another example is that some financial information, such as that relating to Gift Aid, cannot be deleted immediately due to financial auditing regulations.

5. The right to restrict processing

Individuals have the right to restrict processing of their personal data in certain circumstances (for instance if a person believes his/her personal data is inaccurate or he/she objects to the processing). If processing is restricted, you can still store the data but cannot otherwise use the data.

6. The right to data portability

Data subjects will have the right to request that their personal data be provided to them (or a third party) in a machine readable portable format free of charge. The organisation will need to comply with such requests without undue delay, and in any event within one month.

This is a new right introduced by the GDPR. Individuals have the right to obtain and reuse personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT system to another.

7. The right to object

Individuals have the right to object to processing in certain circumstances - e.g. if the LLP has relied on legitimate interest to process data without consent and an individual is not happy with this they have the right to object to LLP processing their data.

8. The right not to be subject to automated decision-making including profiling

The GDPR provides protection against the risk that a potentially damaging decision is taken without human intervention.

APPENDIX 3: Data Audit

All individuals who hold, handle or otherwise process data within or on behalf of AON LLP must complete the following and forward it to the **Data Protection Compliance Manager**.

Important:

- 'Data' is any information about a living person that could identify them. This includes phone numbers and email addresses.
- 'Processing' is doing anything at all with that data – reading or altering or moving it either on a computer or on paper records.
- If data holding or processing changes subsequently, a revised audit form must be submitted.

1.	Name of person holding data:	
2.	Role:	
3.	Data controller:	AON LLP
4.	**PERSONAL COMMUNICATIONS DATA** DATA SUBJECTS: a) Staff b) Suppliers c) Enquirer/Correspondent d) Relative/guardian of a subject e) Child <16 f) Member g) Other:_____ CLASSES OF DATA: a) Personal details b) Social circumstances c) Employment d) Financial e) Ethnicity f) Political g) Religious h) Trade union i) Health – physical/mental j) Sexual life k) Criminal matters l) Education m) Other:_____ Data source(s) ?	

(Eg Individuals themselves)

What is the purpose?
(Eg legal requirement)

Who is information disclosed to?
a) The Data Subjects themselves
b) Relatives/guardians of subjects
c) Prospective employer
d) Employees of the data controller
e) Educational establishment
f) Suppliers
g) Person making enquiry
h) A charitable organization
i) Religious organization
j) The regulatory authorities (eg PVG)
k) Other: _____

Any overseas communications?
a) UK only
b) EEA only
c) Worldwide – which countries?
_____
(includes overseas based data storage/cloud)

5. DATA ON OTHER ORGANISATIONS

Who do we keep personal information on?

What type of information?

Data sources?

What is the purpose?

6 DATA STORAGE

a) How is data stored?

b) What steps have we taken to prevent unauthorized access?

c) How do we allow authorised access?

7	**DELETION/CORRECTION** What is the mechanism for processing a request to delete or correct data?
8	**DATA USE** Are we aware of any data being used for purposes other than that for which it was gathered? Does any third party process data for us (eg an email engine)?
9	**DATA FORMATS** Detail the formats are used for personal data (not already covered above). . (a) computer networks and connections . (b) CCTV and access control systems . (c) communications systems . (d) remote access systems . (e) email and instant messaging systems . (f) telephones, voicemail, mobile phone records . (g) intranet and Internet facilities . (h) paper records
10	**ANY OTHER INFORMATION** **Signed:** Date completed:

APPENDIX 4: Data Consent form: AON LLP

Your privacy is important to us. We would like to communicate with you about AON and its activities. To comply with the General Data Protection Regulations 2018, we need your consent to do this.

Please fill in your name and address and other contact information below and confirm your consent by ticking the boxes below. Every adult and young adult over 13 will need to complete their own form. A parent with parental responsibility will need to complete a form for each child. You can find out more about how we use your personal data by reading our privacy notice which is attached to this form.

Name .....

Address ....

Name of parent: ..... (If you are aged 13 or under your parent or guardian should fill in their name and sign below to confirm their consent).

Please confirm your consent to one or more of the following:

☐**Newsletters & Communications** We may contact you to keep you informed about what is going on including news, events, meetings, groups and activities. These communications may also sometimes appear on our website or in printed or electronic form (including social media).

☐**Activities and groups** We may contact you about groups and activities you may be interested in participating in. We sometimes work with similar groups who are not part of our LLP.

☐Occasionally names and photos may appear in newsletters, bulletins or on websites, or social media. Please indicate if you would be agreeable to this.

Keeping in touch:

☐ Yes please, I would like to receive communications by email

☐ Yes please, I would like to receive communications by telephone

☐ Yes please, I would like to receive communications by mobile phone including text message

☐ Yes please, I would like to receive communications by social media

☐ Yes please, I would like to receive communications by post

Signature ..... Date: _____

Note:

You can grant consent to all the purposes; one of the purposes or none of the purposes. Where you do not grant consent we will not be able to use your personal data; (so for example we may not be able to let you know about forthcoming services and events); except in certain limited situations, such as where required to do so by law or protect members of the public from serious harm. You can find out more about how we use your data from our "Privacy Notice". You can withdraw or change your consent at any time by contacting the AON office.

APPENDIX 5: GENERAL PRIVACY NOTICE

How AON LLP ('we') use you information

AON LLP are committed to safeguarding your personal information. In order to handle 'personal data' about you we are required by law to provide this notice to you.

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. The processing of personal data is governed by *[the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the "GDPR" and other legislation relating to personal data and rights such as the Human Rights Act 1998*].

Why are we collecting your data?

We collect personal data to provide appropriate services, to monitor and assess the quality of our services, to fulfil our purposes as a health care providing organisation and to comply with the law regarding data sharing. In legal terms this is called 'legitimate interests'. When it is required, we may also ask you for your consent to process your data. We do not share your information with others except as described in this notice.

What data do we process?

When we hold or use your information it is known as 'processing'. We will process some or all of the following where necessary to fulfill our roles and responsibilities as an LLP:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to our business, or where you provide them to us, we may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependents;
- Where you make donations or pay for activities, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The data we process is likely to constitute sensitive personal data because, as a medical care provider, the fact that we process your data at all may be suggestive that you have a medical need.
- Where you provide this information, we may also process data from the other categories of sensitive personal data (these are defined as: racial or ethnic origin, sex

life, mental and physical health, details of injuries, medication/treatment received, political beliefs, labour union affiliation, genetic data, biometric data, data concerning sexual orientation and criminal records, fines and other similar judicial records).

How do we process your personal data?

We will comply with the legal obligations to keep personal data up to date; to store and destroy it securely; to not collect or retain excessive amounts of data; to keep personal data secure, and to protect personal data from loss, misuse, unauthorised access and disclosure and to ensure that appropriate technical measures are in place to protect personal data.

We use your personal data for some or all of the following purposes:

- To enable us to meet all legal and statutory obligations;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments;
- To carry out any other voluntary or charitable activities;
- To maintain our own accounts and records;
- To process a payment that you have made;
- To seek your views or comments;
- To notify you of changes to our events and role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising activities;
- To enable us to provide a voluntary service for the benefit of the public;
- Our processing also includes the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for us processing your personal data?

Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party (such as our billing agents, Trust Health or our software providers, Bluespier). We will always take into account your interests, rights and freedoms. Some of our processing is necessary for compliance with a legal obligation. We may also process data if it is necessary for the performance of a contract

with you, or to take steps to enter into a contract.

Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

Sharing your personal data

Your personal data will be treated as strictly confidential. It will only be shared with third parties where it is legally required or where you first give us your prior consent. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- Our administrative/billing partners: Trust health
- Our agents, servants and contractors. For example, we may ask a commercial provider to send out newsletters on our behalf, or to maintain our database software;
- Other persons or practitioners operating with permission within the LLP;
- On occasion, other agencies with which we are carrying out joint events or activities.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavour to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data: When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. The right to access information we hold on you

    a. At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.
    b. There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee.

2. The right to correct and update the information we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us

and your data will be updated.

3. The right to have your information erased.

- If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold. When we receive your request we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).

4. The right to object to processing of your data

- You have the right to request that we stop processing your data. Upon receiving the request we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.

5. The right to data portability

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.

- You can withdraw your consent easily by telephone, email, or by post (to the LLP office).

7. The right to object to the processing of personal data where applicable.

8. The right to lodge a complaint with the Information Commissioner's Office.

Transfer of Data Abroad

Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and

whenever necessary, we will seek your prior consent to the new processing.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the information we hold about you or to exercise all relevant rights, queries or complaints:

The AON Office

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

APPENDIX 6: SPECIFIED ROLE PRIVACY NOTICE

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. The processing of personal data is governed by *[the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the "GDPR" and other legislation relating to personal data and rights such as the Human Rights Act 1998*].

Who are we?

This Privacy Notice is provided to you by AON LLP which is the data controller for your data.

How do we process your personal data?

The data controllers will comply with their legal obligations to keep personal data up to date; to store and destroy it securely; to not collect or retain excessive amounts of data; to keep personal data secure, and to protect personal data from loss, misuse, unauthorised access and disclosure and to ensure that appropriate technical measures are in place to protect personal data. We use your personal data for some or all of the following purposes: -

- To enable us to meet all legal and statutory obligations.
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments;
- To administer our staff records;
- To promote the interests of the LLP;
- To manage our employees and volunteers;
- To maintain our own accounts and records;
- To seek your views or comments;
- To notify you of changes to our events and role holders
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising

activities;

- We will process data about role holders for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations, for example to pay role-holders, monitor their performance and to confer benefits in connection with your engagement as a Role Holder. “Role Holders” includes volunteers, employees, contractors, agents, staff, retirees, temporary employees, beneficiaries, workers, treasurers and other role holders.

- We may process sensitive personal data relating to Role Holders including, as appropriate:

- information about a Role Holder's physical or mental health or condition in order to monitor sick leave and take decisions as to the Role Holder's fitness for work;

- the Role Holder's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;

- in order to comply with legal requirements and obligations to third parties.

- Our processing also includes the use of CCTV systems for the prevention and prosecution of crime.

What data do the data controllers listed above process?

- Names, titles, and aliases, photographs.

- Contact details such as telephone numbers, addresses, and email addresses.

- Where they are relevant to our business, or where you provide them to us, we may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, employment details, hobbies, family composition, and dependents.

- Non-financial identifiers such as passport numbers, driving license numbers, vehicle registration numbers, taxpayer identification numbers, employee identification numbers, tax reference codes, and national insurance numbers.

- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.

- Financial information such as salary, bonus, record of earnings, tax code, tax and benefits contributions, expenses claimed, creditworthiness, car allowance (if applicable), amounts insured, and amounts claimed.

- Other operational personal data created, obtained, or otherwise processed in the

course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.

- Other employee data (not covered above) relating to Role Holders including emergency contact information; gender, birth date, referral source (e.g. agency, employee referral); level, performance management information, languages and proficiency; licences/certificates, citizenship, immigration status; employment status, retirement date; billing rates, office location, practice and speciality; publication and awards for articles, books etc.; prior job history, employment references and personal biographies.

The data we process is likely to constitute sensitive personal data because, as a medical care provider, the fact that we process your data at all may be suggestive of a medical need. Where you provide this information, we may also process other categories of sensitive personal data (These are: racial or ethnic origin, sex life, mental and physical health, details of injuries, medication/treatment received, political beliefs, labour union affiliation, genetic data, biometric data, data concerning sexual orientation and criminal records, fines and other similar judicial records.)

What is the legal basis for processing your personal data?

Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party (such as our administrators, Trust Health or BMI Albyn Hospital). An example of this would be our safeguarding work to protect children and adults at risk. We will always take into account your interests, rights and freedoms.
Some of our processing is necessary for compliance with a legal obligation. We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. We will also process your data in order to assist you in fulfilling your role in the LLP or if processing is necessary for compliance with a legal obligation. Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

Sharing your personal data

Your personal data will be treated as strictly confidential. It will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with

- The appropriate bodies of Trust Health, BMI Albyn Hospital including the other data controllers;

- Our agents, servants and contractors. For example, we may ask a commercial provider to send out newsletters on our behalf, or to maintain our database software;

- Other persons or organisations operating with permission and within the LLP

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavour to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data: -

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. The right to access information we hold on you

- At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.

- There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee .

2. The right to correct and update the information we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. The right to have your information erased

- If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.

- When we receive your request we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).

4. The right to object to processing of your data

- You have the right to request that we stop processing your data. Upon receiving the request we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring

or defend legal claims.

5. The right to data portability

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.

- You can withdraw your consent easily by telephone, email, or by post (the AON Office).

- Note, by invoking this right there is a possibility that you may not be able to undertake your role.

7. The right to object to the processing of personal data where applicable.

8. The right to lodge a complaint with the Information Commissioners Office.

Transfer of Data Abroad

Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review. This Notice was last updated in March 2018.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the information we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, AON LLP

Email:

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

APPENDIX 7: Specified roles register

The undersigned confirm that they have received and understand the requirements of the General Data Protection Regulations as they pertain to their specific role:

YEAR: 20_ _

Name	Role	Signature

Appendix 8: Data breach record

BREACH RECORD	AON LLP
Name of subject	
Data breach scope	
Date of breach	
Impact assessment	
Mitigations/Actions	
Date & time subject notified	
Date and time ICO notified	
Policy review?	
Subsequent communications	
Recorded by:	

APPENDIX 9: Data protection Impact Assessment

A DPIA assesses the impact of any proposed processing operation, for example the use of new technology, on the protection of personal data when processing is likely to result in a high risk to the rights and freedoms of data subjects. A DPIA should be carried out before the processing of the personal data starts and then updated throughout the lifetime of any project. The ICO has produced a 51-page Code of Practice on PIAs, (https://ico.org.uk/media/for- organisations/documents/1595/pia-code-of-practice.pdf).

If two or more of the following apply, it is likely that you will be required to carry out a DPIA. This does not apply to existing systems but would apply if we introduced a new system.

a. Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests.
b. Automated-decision making. Example: when processing leads to the potential exclusion of individuals.
c. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects.
d. Sensitive data. Examples: information about individuals' political opinions, as well as personal data relating to criminal convictions or offences.
e. Large scale data processing. There is no definition of "large scale". However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed.
f. Linked databases - in other words, data aggregation. Example: two datasets merged together, that could "exceed the reasonable expectations of the user". E.g. you merge your mailing list with another group or association.
g. Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. employee-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients.
h. "New technologies are in use". E.g. use of social media, etc. Data transfers outside of the EU.
i. "Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking.

APPENDIX 10:

Data protection compliance review

This form will be used to spot-check compliance within the LLP

Please tick appropriate box

	Yes	No	N/A
Has the data subject been informed of processing?			
Has the data subject been informed of third parties to whom their data may be provided?			
Has the data subject given their consent to the processing?			
If the data subject has not given consent (or consent is not a sufficient ground for processing) is processing justified by data controller's legitimate interest?			
If the data is sensitive data has the data subject given explicit consent?			
Has the data subject been informed of the purpose(s) for processing?			
Is there a clear ground for processing each item of data?			
Is the information gathered no more than is necessary for the purpose(s)?			
Are steps taken to ensure data is accurate?			
Is there a system of rolling reviews to keep data up to date?			
Is there a data retention policy for this data?			
Is there a justification for retaining the data for the period in question?			
Has the data subject been informed of their right of access?			
Is the level of security applied to the data appropriate to the risks represented by the nature of the data to be protected (give consideration to possibility of theft, malicious damage or corruption including computer viruses, unlawful access, accidental disclosure, loss and destruction)?			
Are those who deal with personal data aware of purposes for which it has been collected?			
Are those who process data aware of parties to whom they can legitimately disclose it?			
Where consultants and contractors have access to the data is there a written statement in place governing their obligations regarding security and use of data?			
Are appropriate measures in place for the secure disposal and/or destruction of personal data no longer required?			
Where applicable has consent of the data subject been obtained to transfer personal data to countries outside the EEA?			

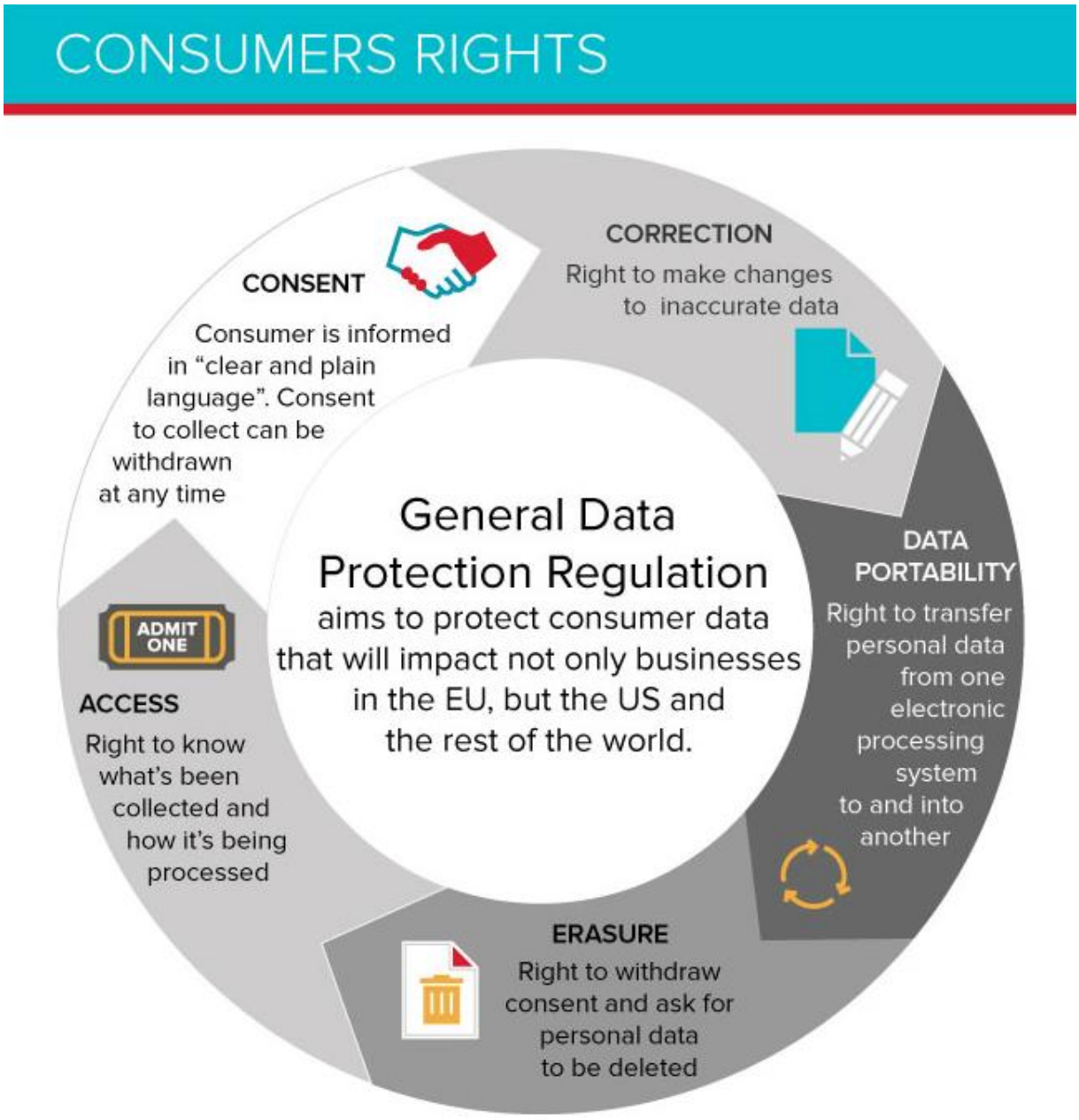
Review carried out on ……..
by……

Appendix XI – Poster for data protection handling areas

AON LLP EMPLOYEES AND DATA HANDLERS – BE AWARE OF GDPR!

CONTACT THE DATA PROTECTION COMPLIANCE MANAGER FOR INFORMATION

AON LLP EMPLOYEES AND DATA HANDLERS – BE AWARE OF GDPR!



AON LLP EMPLOYEES AND DATA HANDLERS – BE AWARE OF WHAT TO DO IN THE EVENT OF A DATA BREACH

- NOTIFY THE DATA PROTECTION COMPLIANCE MANAGER IMMEDIATELY