Ardonagh Specialty General Description of Personal Data Processing

This document contains a general description of all the personal data processing conducted by the various part of Ardonagh Specialty. Typically, business units will process a subset of this data according to their particular specialisms.

Description of Processing

Duration of processing of Personal Data

The duration of processing of the Personal Data are set out in the Ardonagh Specialty data retention standards. Typically, data is retained for 7 years, unless there are legal or regulatory requirements to hold data for longer. Where no contract of insurance is entered into, or where data is processed on a legitimate interests' basis, retention periods will be less than 7 years with personal data being deleted as soon as it is no longer required for its intended purpose.

The categories of Data Subject to whom the Personal Data relates

- Customers and prospective customers of the Ardonagh Group
- Employees (including past and present employees, directors, officers, temporary employees, agents, contractors, secondees, interns and volunteers)

The nature and purpose of the processing of Personal Data

Customer Personal Data

- to assess and provide any products or services requested - this may include a search with a credit reference bureau, or data enrichment services
- to communicate with customers and prospective customers of the Ardonagh Group
- to develop new and existing products and services
- to undertake statistical analysis
- to contact customers about products that are closely related to those already held (either currently or within the last two years) with Ardonagh Group companies
- to provide additional assistance or tips about products or services
- to notify customers of important functionality changes to the Ardonagh websites or other technology services, such as mobile apps
- to provide customers with details of marketing or promotional opportunities and offers relating to other products and services from The Ardonagh Group
- to provide ongoing servicing activities, such as to update customers on the progress of a claim or to discuss renewal of the insurance contract
- to ensure appropriate confidentiality and security of information processed
- to prevent and detect financial crime

- to discharge our regulatory and statutory duties
- marketing and self-promotional activity
- support monitoring and quality management of our employees and processes
- complaint handling
- divestment of business to other parties

Employee Personal Data

- to assess and process job applications (including obtaining references)
- to communicate with employees (including past and present employees, directors, officers, temporary employees, agents, contractors, secondees, interns and volunteers)
- to issue and fulfil any contract of employment or engagement
- to administer the employment or engagement of current and past Staff (including the self-employed, contractors, temporary staff and those on work experience)
- to enable relevant checks and screening to be undertaken to confirm employee identity, eligibility to work and that the employee is a reliable and trustworthy person to undertake your role
- to administer staff services including benefits, payroll, pensions, holidays, training, sickness records, and expenses
- to undertake appraisals and annual review processes
- to arrange secure access to buildings and IT facilities that are necessary
- to provide access to staff services including benefits
- to maintain business continuity plans and emergency contact information
- to undertake planning, strategy development and the management of our work and business
- to deal with disciplinary and grievance matters, staff disputes, and employment tribunals or court litigation
- to ensure that staff are properly supported in their roles, including training
- to obtain occupational health services
- to disclose any information where we are legally obliged to do so
- to protect and further our legitimate interests as an employer and a business
- to detect and prevent fraud or other criminal activity
- to check information against publicly available sources for accuracy

The types of Personal Data to be processed

- *Customers:*

  Name, telephone number, email address, postal address, occupation, date of birth, additional details of risks related to the client enquiry or product and payment details (including bank account number and sort code, premium details, claims details, commission rates and other lifestyle and other risk rating factors).

  Details of complaints; customer opinions on Ardonagh's services; results of market research; and requests to exercise their rights and how these requests were satisfied.

  Details of convictions or medical history as necessary to provide the customer with a product or service or to process a claim.

- *Employees:*

  Name, telephone number, email address, postal address, date of birth and other details (including information obtained during employment, for example, attendance, appraisal or other works records).

  Monitoring information from monitoring systems use and emails, CCTV and certain calls made by staff, all of which may include personal data.

  Details of personal performance; pay and benefits; conflicts of interest; relevant proof of identity; references and qualifications; job title, role and duties; grievances, disputes and disciplinary proceedings; and requests to exercise their rights and how they were satisfied.

  Information in relation to health or medical records and certain other information deemed to be particularly sensitive, such as information collected in the context of equal opportunities monitoring.

Legal basis of processing

This table provide a high-level overview of the legal basis for processing personal data that we use. A record of processing activity is maintained for each business area that contains more details.

Purpose for which we may process your data	**Legal basis for processing this data**
Assess and provide the products or services; this may include a search with a credit reference bureau, or data enrichment services	Processing in connection with a contract
Communicate with you to provide our services, including risk advice	Processing in connection with a contract
Develop new products, systems and services	Legitimate interests
Undertake statistical and risk analysis	This will be on a legitimate interested basis unless we conduct specific work on a contractual basis
Marketing and self-promotional activity	Legitimate interests
Support monitoring and quality management of our employees and processes	Processing in connection with a contract
Complaints	Regulatory obligation (FCA)
Divestment	Contractual
Employee Data	Contractual

High Risk Processing

We do not use systematic and extensive profiling or automated decision-making to make significant decisions about people.

We process the following types of Sensitive personal data in connection with our insurance intermediary activities and the employment of our workforce:

Customers

Details of convictions or medical history as necessary to provide the customer with a product or service or to process a claim.

Employees

Information in relation to health or medical records and certain other information deemed to be particularly sensitive such as ethnicity, religious belief and other equal opportunities monitoring data.

We do not process biometric data.

We do not process genetic data.

We may perform data matching to prevent fraud and enrich risk information about a data subject.

We may conduct invisible processing for direct marketing purposes.

We may conduct tracking activities linked to web browsers, but not individuals in connection with use of our websites and marketing purposes.

We do not target our products or services at children.

We do not process personal data that could result in the realistic risk of physical harm in the event of a security breach.

All potential high-risk processing is subject to a privacy by design process that include a DIPA.

Third Party Processing

We may from time to time procure the services of third parties to conduct the following processing activities for us:

- IT services including support, Infrastructure and Software as a service
- Claims handling
- Printing
- Archival and data storage
- Employee benefits services, including occupational health services
- Data enrichment services
- Data analytics services
- Fraud prevention services
- Employee screening and background checks
- Employee training include apprenticeships

Personal Data Exporting

Based on current supplier and other business relationships, data may be exported to:

1. All non-EEA territories in which the group operates (in respect of central sanctions checking service that is operated by Advisory IT)
2. EEA territories
3. India
4. US
5. Canada
6. Singapore
7. Australia
8. Malaysia
9. Costa Rica

Data Protection and Privacy Framework

Ardonagh Specialty has implemented a data protection framework to protect the privacy, rights and freedoms of the data subjects for which it processes personal data.

Attestations review of policies and business standards take place every 6 months. Senior managers who own policies are the distribution leads for each of our divisions. Certified personals are the distribution leads for each business area of the divisions, plus a separate instance for HR. The Specialty Data Protection Officer supports the framework and attestation process, providing processes, training and SME advice.

Note that DFN refers to our internal risk management system.

Supporting Documents

The most up to date versions of following documents that support our data privacy framework can be sent to interested parties as part of our assurance materials:

- Data Protection Business Standard: https://app.employeeapp.co.uk/page/18020
- Record Keeping Business Standard: https://app.employeeapp.co.uk/page/196
- Ardonagh Specialty Acceptable Use Policy: https://app.employeeapp.co.uk/page/5215

Appendix – Appropriate Policy Document 1 Insurance Purpose

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

The purpose of this section is to demonstrate that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles and will outline your retention policies with respect to this data.

Description of data processed

Medical and criminal convictions data is processed in relation to the placement of insurance policies to enable assessment of risk, and in the administration of claims to validate policy terms when establishing cover and, in the case of medical information, establish the quantum.

Schedule 1 condition for processing

From the DPA 2018 Schedule 1 part 1

Insurance

20(1)This condition is met if the processing—

(a)is necessary for an insurance purpose,

(b)is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health, and

(c)is necessary for reasons of substantial public interest,

subject to sub-paragraphs (2) and (3).

(2)Sub-paragraph (3) applies where—

(a)the processing is not carried out for the purposes of measures or decisions with respect to the data subject, and

(b)the data subject does not have and is not expected to acquire—

(i)rights against, or obligations in relation to, a person who is an insured person under an insurance contract to which the insurance purpose mentioned in sub-paragraph (1)(a) relates, or

(ii)other rights or obligations in connection with such a contract.

(3)Where this sub-paragraph applies, the processing does not meet the condition in sub-paragraph (1) unless, in addition to meeting the requirements in that sub-paragraph, it can reasonably be carried out without the consent of the data subject.

(4)For the purposes of sub-paragraph (3), processing can reasonably be carried out without the consent of the data subject only where—

(a)the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b)the controller is not aware of the data subject withholding consent.

(5)In this paragraph—

- *"insurance contract" means a contract of general insurance or long-term insurance;*
- *"insurance purpose" means—*

  (a) advising on, arranging, underwriting or administering an insurance contract,

  (b) administering a claim under an insurance contract, or

  (c) exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law.

(6)The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

(7)Terms used in the definition of "insurance contract" in sub-paragraph (5) and also in an order made under section 22 of the Financial Services and Markets Act 2000 (regulated activities) have the same meaning in that definition as they have in that order.

Procedures for ensuring compliance with the principles

Accountability principle

i. We maintain appropriate documentation of our processing activities – see DFN Information Asset Register.

ii. We have appropriate data protection policies – See Group Data Protection business standard.

iii. We carry out data protection impact assessments (PIAs) for uses of personal data that are likely to result in high risk to individuals' interests. See PIA Archive.

Principle (a): lawfulness, fairness and transparency

i. We identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data and documented this in our information Asset Register.

ii. We make appropriate privacy information available with respect to the SC/CO data in our Privacy notices. The current standard wording is:

"… We may need to request, collect and process additional sensitive personal information such as, but not limited to, details of convictions or medical history for us to provide you with the product or service or to process a claim. This information will be collected from you as it is considered necessary for a

legitimate insurance purpose and contractual obligations that arise from the provision of insurance products and services to you.

We only collect and process sensitive personal data where it is critical for the delivery of insurance products and services we provide to you and as allowed under UK law. If you object to use of this information, then we will be unable to offer you that product or service."

iii. We open and honest when we collect the SC/CO data, and we ensure that we do not deceive or mislead people about its use. We ask new customers if they wish to have our Privacy Notice explained to them as part of call scripts and include a notice in our terms of business agreements, to ensure that we are transparent in our use of data.

Principle (b): purpose limitation

i. We clearly identified our purpose for processing the SC/CO data and recorded this in our Information Asset Register.

ii. We included appropriate details of these purposes in our privacy information for individuals.

iii. Any plans of a new purpose of use of personal (other than a legal obligation or function set out in law), is checked that this is compatible with our original purpose as part of our privacy by design process. See PIA Triage questions.

Principle (c): data minimisation

i. We are satisfied that we only collect SC/CO personal data we actually need for our specified purposes. A Data minimisation exercise is a mandatory part of our privacy impact assessment.

ii. We are satisfied that we have sufficient SC/CO data to properly fulfil those purposes.

iii. We have processes to periodically review this SC/CO data and delete data that is no longer necessary.

Principle (d): accuracy

i. We have appropriate processes in place to check the accuracy of the SC/CO data we collect, and we record the source of that data. This forms part of our routine quality assurance monitoring process.

ii. We have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and we update it as necessary. Mid-term adjustment and renewal processes required all personal data is reviewed and confirmed accurate by the Data Subject.

iii. We have a policy or set of procedures which outline how we ensure compliance with the individual's rights to rectification and erasure. We have complaints processes and processes to uphold individual rights that address these scenarios.

Principle (e): storage limitation

i. We carefully consider how long we keep the SC/CO data and can we justify this amount of time in our retention schedules. See Specialty retention requirements.

ii. We regularly review our information and erase or anonymise this SC/CO data when we no longer need it. We are implementing processes to routinely enforce our retention requirements.

iii. We do not keep any SC/CO data that we need to keep for public interest archiving. Note that ELTO records are sent to this organisation for archiving.

Principle (f): integrity and confidentiality (security)

i. We have analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data. See group cyber security business standard.

ii. We have an information security policy (or equivalent) regarding this SC/CO data, and we take steps to make sure the policy is implemented. See group cyber security business standard and Group cyber security controls monitoring activity. All group policies are regularly reviewed.

iii. We put other technical measures or controls in place appropriate to the circumstances and the type of SC/CO data we are processing in accordance with the group Cyber business standard.

Retention and erasure policies

We have documented retention requirements for broking activities.

Appendix – Appropriate Policy Document 2 - Employee Medical Data

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

The purpose of this section is to demonstrate that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles and will outline your retention policies with respect to this data.

Description of data processed

Medical data is processed in relation to the management of employees' occupational health needs during the course of their employment. Records are then kept for a statutory period in relation to the contract of employment after leaving the company.

Schedule 1 condition for processing

From the DPA 2018 Schedule 1 part 1

Support for individuals with a particular disability or medical condition

16(1)This condition is met if the processing—

(a)is carried out by a not-for-profit body which provides support to individuals with a particular disability or medical condition,

(b)is of a type of personal data falling within sub-paragraph (2) which relates to an individual falling within sub-paragraph (3),

(c)is necessary for the purposes of—

(i)raising awareness of the disability or medical condition, or

(ii)providing support to individuals falling within sub-paragraph (3) or enabling such individuals to provide support to each other,

(d)can reasonably be carried out without the consent of the data subject, and

(e)is necessary for reasons of substantial public interest.

(2)The following types of personal data fall within this sub-paragraph—

(a)personal data revealing racial or ethnic origin;

(b)genetic data or biometric data;

(c)data concerning health;

(d)personal data concerning an individual's sex life or sexual orientation.

(3)An individual falls within this sub-paragraph if the individual is or has been a member of the body mentioned in sub-paragraph (1)(a) and—

(a)has the disability or condition mentioned there, has had that disability or condition or has a significant risk of developing that disability or condition, or

(b)is a relative or carer of an individual who satisfies paragraph (a) of this sub-paragraph.

(4)For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a)the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b)the controller is not aware of the data subject withholding consent.

(5)In this paragraph—"carer" means an individual who provides or intends to provide care for another individual other than—

(a)under or by virtue of a contract, or

(b) as voluntary work ;"disability" has the same meaning as in the Equality Act 2010 (see section 6 of, and Schedule 1 to, that Act)

.

(6)The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Procedures for ensuring compliance with the principles

Accountability principle

i. We maintain appropriate documentation of our processing activities – see DFN Information Asset Register.

ii. We have appropriate data protection policies – see Group Data Protection business standard.

iii. We carry out data protection impact assessments (PIAs) for uses of personal data that are likely to result in high risk to individuals' interests. See PIA Archive.

Principle (a): lawfulness, fairness and transparency

i. We identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data and documented this in our information Asset Register.

ii. We make appropriate privacy information available with respect to the SC/CO data in our Privacy notices. The current standard wording is:

"… Sometimes we may need to request and collect particularly sensitive information about you. This might include information in relation to your physical and mental health or medical records, and certain other information is also deemed to be particularly sensitive, such as equal opportunities monitoring data. More information can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

Where we need this sensitive information, and the information is not required for your employment, to protect your physical and mental health or equal opportunities we will obtain your explicit consent to process this information. If we are processing your data on the basis of your consent, you may withdraw that consent at any time. Please note that typically we process data on basis that it relates to a contract of employment or another legal basis of processing, so this right will not be applicable in many instances.

… In the event of an emergency, and only where we believe there is a risk of serious harm to you or others, we may share relevant information we hold about your physical or mental health with emergency services, health services or next of kin."

iii. We open and honest when we collect the SC/CO data, and we ensure that we do not deceive or mislead people about its use. We provide transparency notices to candidates are the time or application, to successful candidate along with their offer of employment, to employees via our intranet.

Principle (b): purpose limitation

i. We have clearly identified our purpose for processing the SC/CO data and recorded this in our Information Asset Register.

ii. We included appropriate details of these purposes in our privacy information for individuals. This purpose is clearly stated in our employee transparency notices.

iii. Any plans of a new purpose of use of personal (other than a legal obligation or function set out in law), is checked that this is compatible with our original purpose as part of our privacy by design process. See PIA Triage questions.

Principle (c): data minimisation

i. We are satisfied that we only collect SC/CO personal data we actually need for our specified purposes. A Data minimisation exercise is a mandatory part of our privacy impact assessment.

ii. We are satisfied that we have sufficient SC/CO data to properly fulfil those purposes.

iii. We have processes to periodically review this SC/CO data and delete data that is no longer necessary.

Principle (d): accuracy

i. We have appropriate processes in place to check the accuracy of the SC/CO data we collect, and we record the source of that data. This forms part of our routine quality assurance monitoring process.

ii. We have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and we update it as necessary. Staff are regularly encouraged to keep their personal information updated and to inform us of health issues.

iii. We have a policy or set of procedures which outline how we ensure compliance with the individual's rights to rectification and erasure. We have complaints and HR grievance processes and processes to uphold individual rights that address these scenarios.

Principle (e): storage limitation

i. We carefully consider how long we keep the SC/CO data and can we justify this amount of time in our retention schedules. See Specialty retention requirements.

ii. We regularly review our information and erase or anonymise this SC/CO data when we no longer need it. We are implementing processes to routinely enforce our retention requirements.

iii. We do not keep any SC/CO data that we need to keep for public interest archiving.

Principle (f): integrity and confidentiality (security)

i. We have analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data. See group cyber security business standard.

ii. We have an information security policy (or equivalent) regarding this SC/CO data, and we take steps to make sure the policy is implemented. See group cyber security business standard and Group cyber security controls monitoring activity. All group policies are regularly reviewed.

iii. We put other technical measures or controls in place appropriate to the circumstances and the type of SC/CO data we are processing in accordance with the group Cyber business standard.

Retention and erasure policies

We have documented retention requirements for broking activities.

Appendix – Appropriate Policy Document 3 – Equal Opportunity Data

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

The purpose of this section is to demonstrate that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles and will outline your retention policies with respect to this data.

Description of data processed

Medical data is processed in relation to the management of employees' occupational health needs during the course of their employment. Records are then kept for a statutory period in relation to the contract of employment after leaving the company.

Schedule 1 condition for processing

Equality of opportunity or treatment

8(1)This condition is met if the processing—

(a)is of a specified category of personal data, and

(b)is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained,

subject to the exceptions in sub-paragraphs (3) to (5).

(2)In sub-paragraph (1), "specified" means specified in the following table—

Category of personal data	*Groups of people (in relation to a category of personal data)*
Personal data revealing racial or ethnic origin	People of different racial or ethnic origins
Personal data revealing religious or philosophical beliefs	People holding different religious or philosophical beliefs
Data concerning health	People with different states of physical or mental health
Personal data concerning an individual's sexual orientation	People of different sexual orientation

(3)Processing does not meet the condition in sub-paragraph (1) if it is carried out for the purposes of measures or decisions with respect to a particular data subject.

(4)Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(5)Processing does not meet the condition in sub-paragraph (1) if—

(a)an individual who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject (and has not given notice in writing withdrawing that requirement),

(b)the notice gave the controller a reasonable period in which to stop processing such data, and

(c)that period has ended.

Racial and ethnic diversity at senior levels of organisations

9(1)This condition is met if the processing—

(a)is of personal data revealing racial or ethnic origin,

(b)is carried out as part of a process of identifying suitable individuals to hold senior positions in a particular organisation, a type of organisation or organisations generally,

(c)is necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation or organisations, and

(d)can reasonably be carried out without the consent of the data subject,

subject to the exception in sub-paragraph (3).

(2)For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a)the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b)the controller is not aware of the data subject withholding consent.

(3)Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(4)For the purposes of this paragraph, an individual holds a senior position in an organisation if the individual—

(a)holds a position listed in sub-paragraph (5), or

(b)does not hold such a position but is a senior manager of the organisation.

(5)Those positions are—

(a)a director, secretary or other similar officer of a body corporate;

(b)a member of a limited liability partnership;

(c)a partner in a partnership within the Partnership Act 1890, a limited partnership registered under the Limited Partnerships Act 1907 or an entity of a similar character formed under the law of a country or territory outside the United Kingdom.

(6)In this paragraph, "senior manager", in relation to an organisation, means a person who plays a significant role in—

(a)the making of decisions about how the whole or a substantial part of the organisation's activities are to be managed or organised, or

(b)the actual managing or organising of the whole or a substantial part of those activities.

(7)The reference in sub-paragraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

Procedures for ensuring compliance with the principles

Accountability principle

i. We maintain appropriate documentation of our processing activities – see DFN Information Asset Register.

ii. We have appropriate data protection policies – see Group Data Protection business standard.

iii. We carry out data protection impact assessments (PIAs) for uses of personal data that are likely to result in high risk to individuals' interests. See PIA Archive.

Principle (a): lawfulness, fairness and transparency

i. We identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data and documented this in our information Asset Register.

ii. We make appropriate privacy information available with respect to the SC/CO data in our Privacy notices. The current standard wording is:

"… Sometimes we may need to request and collect particularly sensitive information about you. This might include information in relation to your physical and mental health or medical records, and certain other information is also deemed to be particularly sensitive, such as equal opportunities monitoring data. More information can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

Where we need this sensitive information, and the information is not required for your employment, to protect your physical and mental health or equal opportunities we will obtain your explicit consent to process this information. If we are processing your data on the basis of your consent, you may withdraw that consent at any time. Please note that typically we process data on basis that it relates to a contract of employment or another legal basis of processing, so this right will not be applicable in many instances."

iii. We open and honest when we collect the SC/CO data, and we ensure that we do not deceive or mislead people about its use. We provide transparency notices to candidates are the time or application, to successful candidate along with their offer of employment, to employees via our intranet.

Principle (b): purpose limitation

i. We have clearly identified our purpose for processing the SC/CO data and recorded this in our Information Asset Register.

ii. We included appropriate details of these purposes in our privacy information for individuals. This purpose is clearly stated in our employee transparency notices.

iii. Any plans of a new purpose of use of personal (other than a legal obligation or function set out in law), is checked that this is compatible with our original purpose as part of our privacy by design process. See PIA Triage questions.

Principle (c): data minimisation

i. We are satisfied that we only collect SC/CO personal data we actually need for our specified purposes. A Data minimisation exercise is a mandatory part of our privacy impact assessment.

ii. We are satisfied that we have sufficient SC/CO data to properly fulfil those purposes.

iii. We have processes to periodically review this SC/CO data and delete data that is no longer necessary.

Principle (d): accuracy

i. We have appropriate processes in place to check the accuracy of the SC/CO data we collect, and we record the source of that data. We have an annual campaign to encourage employees to keep their personal information updated and regularly review and report on the quality of this data.

ii. We have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and we update it as necessary. Staff are regularly encouraged to keep their personal information updated and to inform us of health issues.

iii. We have a policy or set of procedures which outline how we ensure compliance with the individual's rights to rectification and erasure. We have complaints and HR grievance processes and processes to uphold individual rights that address these scenarios.

Principle (e): storage limitation

i. We carefully consider how long we keep the SC/CO data and can we justify this amount of time in our retention schedules. See Specialty retention requirements.