Age Check
Certification Scheme

Technical Requirements for Data Protection and Privacy

ACCS 2: 2021



Age Check Certification Services Ltd

UKAS PRODUCT CERTIFICATION 21037

© Age Check Certification Scheme Ltd (2021) All Rights Reserved



This is a publicly available specification created by the Age Check Certification Scheme Ltd. It is subject to the intellectual property rights of the Scheme and may not be copied, used in a retrieval system or utilised without the express consent of the Scheme, save that it may be mentioned by name as a reference document with appropriate attribution and a link to the document itself.
© Age Check Certification Scheme Ltd 2021. All rights reserved.

The certification criteria contained within this document have been approved by the Information Commissioner's Office in accordance with the Commissioner's tasks and powers under Articles 57(1)(n) and 58(3)(f) pursuant to Article 42(5) of the UK General Data Protection Regulation.





© Age Check Certification Scheme

Contents

Introduction 4

1. Scope 7

- Scope of Scheme Criteria for Age Check Services 8
- Types of Age Check Services in Scope 9
- Types of Service Provided by Age Check Services in Scope 9
- Types of Data Processing by Age Check Services in Scope 10
- Processing by Age Check Services Not In Scope 11
- Target of Evaluation for Age Check Services 12
- Territorial Scope for Age Check Services 13

2. Normative References 15

- Age Check Certification Scheme 16
- Legal Provisions 16
- National and International Standards 17
- Other Documents 18

3. Terms and Definitions 21

4. Data Protection Management Systems 29

- Leadership and Oversight of Data Protection Responsibilities 30
- Age Check Practice Statement 33
- Data Protection Policies 34
- Information Security and Risk Management 37
- Data Protection Officers 40
- Data Protection Impact Assessment (DPIA) 41
- Training and Awareness for Staff and Contractors 43
- Sub-contractors and External Providers Processing Personal Data 45
- Managing Personal Data Breaches 47

5. Requirements for Data Processing 51

- Data Protection by Design and Default 52
- Lawful Basis of Processing 52
- Fairness 52
- Consent 53
- Contract 54
- Legal Obligation 55
- Vital Interests 56
- Public Tasks 56

Legitimate Interests 56
Purpose Limitation 57
Data Minimisation 58
Accuracy 59
Storage Limitation 61
Data Subject Rights 63
Right to Be Informed (Privacy Policy) 63
The Right of Access 65
The Right to Rectification 67
The Right to Erasure 68
The Right to Restrict Processing 69
The Right to Data Portability 70
The Right to Object 71
Rights in Relation to Automated Decision Making and Profiling 72
Transparency 75
Special Category Data and Biometrics 76
International Transfers 78
Data Sharing 79
6. Technical Evaluation 83
Test Protocols (Method of Evaluation) 84
Penetration Testing 85

Introduction

The Age Check Certification Scheme tests that age check systems work. There are a wide range of businesses that have to take steps to gain assurance about the age of their customers, particularly if they are selling age restricted goods, content or services or information society services providing age appropriate design. These businesses tend to use service providers such as Proof-of-Age ID Providers, Age Check Providers, Age Exchange Service Providers, Electronic ID Validation Services and Analytical and Profiling Services.

These technical requirements have been developed in response to public concern, campaigns and industry needs highlighted about the handling, privacy and security of personal data when going through an age assurance process or designing age appropriate services.

The Scheme is operated through our UKAS accredited conformity assessment body (Age Check Certification Services Ltd) and the certification criteria contained within this document have been approved by the Information Commissioner's Office in accordance with the Commissioner's tasks and powers under Articles 57(1)(n) and 58(3)(f) pursuant to Article 42(5) of the UK GDPR.

Data protection and privacy is critical to the successful operation of age check data processing services and when designing age appropriate services. These technical requirements form an essential (and mandatory) part of the assessment of the efficacy and accuracy of clients' age check processes or age appropriate design. So these technical requirements stand alongside the International and National Standards, local Standards and other technical requirements operated by the Scheme. These are all listed in Section 2 of this document (Normative References).

This document defines the technical, organisational and documentary requirements, including data protection enhancement techniques, specifically for providers of age check services or providers of age restricted goods, services or content, or design of information society services likely to be accessed by children and related to privacy, handling of personal data and the obligations arising from UK GDPR.

In addition, children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguarding concerns and their rights in relation to the processing of personal data. Any information given to, or provided in communication with, a child shall be in "such a clear and plain language that the child can easily understand". Where a child asks a business to provide a service for which payment is normally made, parental consent shall be required unless the child is aged 16 years or over. These technical requirements recognise that organisations carrying out age assessments have particular responsibilities when handling data that they identify as being the personal data of a child.

Any certification against the Age Check Certification Scheme does not reduce the responsibility of the data controller or the data processor to comply with UK GDPR and is without prejudice to the tasks and powers of the Information Commissioner's Office.

These technical requirements are applicable to any organisation described in Section 1 (Scope), regardless of size, type and nature, and applies to its activities, products and services involving personal data processing, that the organisation can control or influence considering a life cycle of the data processing.

The Age Check Certification Scheme Rules and Procedures also set out the requirements for Scheme Clients and commitments to Age Verification and Design Best Practice. This document then sets out the rules that are applicable to all clients, and those applicable to clients applying for all types of age checking services, to relying parties in connection with their data processing activities or to information society services in relation to the age appropriate design of their services.

The Age Check Certification Scheme Rules and these technical requirements have been designed to comply with ISO/IEC 17065:2012, the UK Information Commissioner's additional accreditation requirements for certification bodies, the relevant regulatory requirements for age verification service providers, the provisions of UK GDPR, the appropriate product and service standards and the requirements of the Trade Mark Rules 2008.

PLEASE NOTE: Scheme Clients cannot apply for UK GDPR certification on its own through this scheme, they must be applying for certification against the technical requirements directly relevant to their business activities (such as 'Age Estimation Technologies' as an example). Assessment against these technical requirements for data protection and privacy is automatically included in order to gain UK GDPR certification.





Scope



1. Scope

1.1 The suite of Age Check Certification Scheme (ACCS) Technical Requirements (described in Section 2 – Normative References) are applicable to Scheme Clients submitting their products, processes or services for certification from ACCS. These technical requirements specifically cover the processing of personal data within those products, processes or services as the object of the UK GDPR certification. Scheme Clients that can demonstrate compliance with the technical requirements and gain certification are entitled to use the scheme logo (mark of conformity) on their promotional material.

PLEASE NOTE: The Scope of the Scheme Criteria and Target of Evaluation for Age Appropriate Design of Information Society Services is set out in Section 1 of ACCS 3. Those technical requirements apply certain aspects of this document to avoid unnecessary duplication. The Scope of Scheme Criteria in this document focusses on Age Check Services.

Scope of Scheme Criteria for Age Check Services

1.2 These technical requirements set out the specific data processing requirements for activities concerned with the processing of personal data when undertaking age check practices, covering the relevant phases of processing and the whole life-cycle of data including:

a) Age check policies – including deletion and/or anonymisation

b) Data Creation, Data storage, data usage, data archival and data destruction

c) Data privacy, protection and security

d) Technical organisational measures, including information security management, vulnerability scanning and penetration testing

e) Data subject rights, including access to privacy policies, access to information, rights to rectification, erasure, restricting processing, data portability and rights to object

f) Automated decision-making and profiling of personal data

g) The roles of Data Protection Officers and preparation of Data Protection Impact Assessments

h) Sub-contracting of processing activities, including the use of age attribute exchanges and contract specifications

i) Age attributes, including checking processes for age attributes, scoring and assessment

1.3 Any Scheme Client that applies for certification under one of the standards or technical requirements applicable to their activities (as set out in Section 2 – Normative Requirements) shall be assessed for their data processing in accordance with these technical requirements.

Types of Age Check Services in Scope

1.4 The scope of these technical requirements covers any of the following types of organisation acting as a data controller or joint data controller, that provide at least one of the services in this section 1.4 undertaking any of the processing activities in section 1.6 but excluding any processing activities in section 1.7, that is any:

a) Proof-of-Age ID Providers that verify age attributes and issue a reusable physical ID card, token or app that an unknown third party (such as a retailer) can rely on with or without a pre-arranged contractual relationship with the Proof-of-Age ID Provider

b) Age Check Providers that verify age attributes on request by a third party on a transaction-by-transaction basis under a pre-arranged contractual relationship with the Age Check Provider

c) Age Check Exchange Providers or Brokers that provide an online gateway for Age Check Providers and Relying Parties to access user asserted, permissioned and verified attributes

d) Relying Parties (online or offline) that rely on results of an age check (either remotely or during a face-to-face encounter) to establish the age-related eligibility of an individual for the purposes of a transaction (such as sellers or providers of age restricted goods and services)

Types of Service Provided by Age Check Services in Scope

1.5 Age Check Providers are likely to be providing at least one of the following services aimed at achieving age assurance about any individual:

a) Age determination – an indication establishing that an individual has a particular age stated to a specified level of confidence and by reference to information related to that individual

b) Age categorisation – an indication establishing that an individual is of an age that is within a category of ages, over a certain age or under a certain age to a specified level of confidence and by reference to information or factors related to that individual

c) Age estimation – an indication by estimation that an individual is likely to fall within a category of ages, over a certain age or under a certain age to a specified level of confidence by reference to inherent features or behaviours related to that individual

Types of Data Processing by Age Check Services in Scope

1.6 To be eligible for certification against the requirements of this Scheme, Clients shall be undertaking one or more of the following data processing activities:

a) Age Attributes - gathering of claimed age attributes and verification of these against a reliable source of authentication

b) Biometric Attributes - processing of biometric or inherent features and analysis of these against a trained data set to make age estimation calculations and which may allow or confirm the unique identification of that natural person, such as facial images or fingerprint data for user enrolment and authentication

c) Personal Identifiable Information – gathering of data from personal identity documents and data sources with a view to extracting age attributes and triangulation of data

d) Customer Records - keeping of customer account records to enable future age verification activities

e) Authentication Tokens - the provision of data packets that provide a user with ongoing authentication records (such as cookies)

f) Special Category Data – including processing of personal data relating to gender, race and disability only in so far as it relates to the determination of whether generic algorithms incorporate inherent bias in age estimation or determination

Note 1: *The types of processing in scope do not cover all types of special category data as defined by UK GDPR.*

g) Profiling - including automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to behaviours of a natural person

h) Pseudonymisation - processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information

i) Consent, including 3rd party parental or guardianship consent – including any processing of data indicating agreement to the processing of personal data relating to him or her or their child or a child that they exercise parental responsibility for

j) Cross-Border Data Processing - where targets of evaluation utilise data resources from outside of the United Kingdom

Processing by Age Check Services Not In Scope

1.7 The Age Check Certification Scheme does not include assessment of processing activities that are not considered to be relevant to the processing activities of Age Check Services such as:

a) the processing of physical or mental health, wellbeing or patient personal data (except in so far as covered by the scope of s.1.6 (f))

b) the processing of criminal records or criminal activity

c) the processing of political opinions, religious or philosophical beliefs

d) the processing of data revealing trade union membership

e) the processing of genetic data – in particular unique information about a natural person's inherited or acquired genetic characteristics

f) the processing of a natural person's sex life or sexual orientation – in particular the scheme prohibits processing of personal data or augmentation of personal data with other data that may reveal a natural person's sex life or sexual orientation (such as online browsing habits)

g) the processing of a natural person's data for profiling of performance at work, economic situation, health, personal preferences, interests, reliability, location or movements

h) the processing of data for the purposes of direct marketing

i) the processing of data purely as a data processor

Note 1: *In order to be regarded as purely a data processor all of the following statements shall be true:*

a) They follow instructions from someone else regarding the processing of personal data and make none of their own decisions in that respect

b) They are given the personal data by their customer or a similar third party or are told by that customer or similar third party what data to collect

c) They do not decide themselves to collect personal data from individuals

d) They do not make any decisions themselves about the lawful basis of use of that data

e) They do not decide what purpose or purposes that the data will be used for

f) They do not decide whether to disclose the data, or to whom

g) They do not decide how long to retain the data

h) The decisions about how the data is processed are prescribed in a contract with someone else and the decisions made about data processing by the Scheme Client are merely related to the implementation of that contract

i) They have no interest in the end result of the data processing

***Note 2:** Whilst it is not impossible that an Age Check Provider is acting purely as a data processor on behalf of its clients, it is unlikely to be true in all circumstances. As such, it is important for organisations that regard themselves as being merely data processors to have clear written contracts and policies about entering into such contracts that maintain their status as data processors.*

Target of Evaluation for Age Check Services

1.8 The Target of Evaluation is all processing of personal data by the Scheme Client's age assurance process relating to the gathering of the initial claim of age attribute through to the determination, categorisation and estimation of the authenticity of the claimed age attribute. The Target of Evaluation may also cover the future processing of an individual age attribute or personal identifiable information for the purpose of reverification or customer relationship management.

1.9 The Target of Evaluation shall define the targeted processing operation in terms of data types, systems and processes used. This needs to define where the processing subject to evaluation starts and ends, including any interfaces and interdependent processing operations, including any processing on shared or externally hosted systems or by data processors acting on behalf of the Scheme Client. It shall also identify all relevant processing operations including an illustration of data flows, the area of application and reflect any special types of processing (e.g. automated decision making, profiling, high risk processing).

1.10 The Target of Evaluation shall define any interfaces or interdependent processing that is outside of the scope of the Scheme which shall be excluded from the Target of Evaluation. The Scheme Client shall provide an explanation for justifying any inclusion or exclusion of aspects of their data processing from the scope of certification.

1.11 An accurate specification of the Target of Evaluation is of fundamental importance for the certification procedure as it decides on what is covered by the certification. The Target of Evaluation shall be described on the Certification Documentation.

1.12 The Target of Evaluation shall include the identification of any processing of special category data (such as inherent or biometric features). Section 5.9 sets out specific requirements in relation to the handling of special category data.

1.13 The relevant scope set out above shall be determined for each age check system or process submitted for evaluation as a part of the application review process.

Note 1: *The Target of Evaluation for Information Society Services submitted applications under ACCS 3 – Technical Requirements for Age Appropriate Design is set out in ss 1.12 – 1.15 of ACCS 3.*

Territorial Scope for Age Check Services

1.14 The UK GDPR Certification Scheme is applicable to where:

a) the data processing activities are conducted by organisations (controller or processor) established in the United Kingdom; or

b) the data processing activities relate to the offering of goods or services (even if for free) to data subjects situated in the United Kingdom (not restricted to those individuals).

Note 1: *Monitoring of behaviour of data subjects in the UK is out of scope for this scheme.*

1.15 Scheme Clients that are non-UK organisations shall appoint a UK representative, with a mandate of authority to act on behalf of the Scheme Client in the UK. The UK representative may be an individual, or a company or organisation established in the UK, and shall be able to represent the Scheme Client regarding their obligations under the UK GDPR (e.g. a law firm, consultancy or private company).





2

Normative Refernces

Normative References



2. Normative References

Age Check Certification Scheme

The Age Check Certification Scheme is built on a modular approach to applicable standards and technical requirements. As a part of the Application Review Process, a Certification Officer assesses the applicable requirements for the business model of the Scheme Client. The suite of applicable requirements is constantly changing as new methodologies emerge, new standards are developed and new technical requirements are introduced. A full comprehensive current list can be found on the Standards Section of the Scheme website, but include:

ACCS 0: 2021 – General Scheme Rules (covering the process of certification under ISO 17065:2012)

ACCS 1: 2020 – Technical Requirements for Age Estimation Technologies

ACCS 2: 2021 – Technical Requirements for Data Protection and Privacy*

ACCS 3: 2021 – Technical Requirements for Age Appropriate Design for Information Society Services*

ACCS 4: 2020 – Technical Requirements for Age Check Providers

ACCS 5: 2021 – Technical Requirements for Age Check System Penetration Testing and Vulnerability Scans (In Development)

ACCS 6: 2021 – Technical Requirements for Parental Consent or Social Proofing for Age Gateway Technologies (In Development)

** **ACCS 2:2021** and **ACCS 3:2021** are technical requirements that have been approved by the Information Commissioner's Office in accordance with the Commissioner's tasks and powers under Articles 57(1)(n) and 58(3)(f) pursuant to Article 42(5) of the UK GDPR.*

Legal Provisions

The process of gaining age assurance is governed by numerous statutes and legal provisions relating to the control of access to age restricted goods, content and services. In addition to these, there are specific legal provisions relevant to the operation of the technical requirements in this document:

- Borders, Citizenship and Immigration Act 2009
- Data Protection Act 2018
- Electronic Identification, Authentication and Trust Services Regulation (EU) 2014/910
- General Data Protection Regulation (EU) 2016/679 as it applies in the United Kingdom by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 as amended

- Modern Slavery Act 2015

National and International Standards

BS ISO/IEC 7810:2019 – Identification cards – Physical characteristics

ISO 17065:2012 – Conformity assessment – Requirements for bodies certifying products, processes and services

ISO/IEC 19794-5:2011 + A2:2015 – Information technology – Biometric data interchange formats – Part 5: Face image data

ISO/IEC 19795-1:2006 – Information technology – Biometric performance testing and reporting – Part 1: Principles and framework

ISO 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 29100:2011 – Information technology – Security techniques – Privacy

ISO/IEC 29101:2013 – Information technology – Security techniques – Privacy architecture framework

ISO/IEC 29109-5:2019 – Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 Part 5: Face image data

ISO/IEC 29115:2013 – Information technology – Security techniques – Entity authentication assurance framework

ISO/IEC 30107-1:2016 – Information technology – Biometric presentation attack detection

ISO 9001:2015 – Quality management systems – Requirements

PAS 1296:2018 – Code of Practice for Age Check Services

PASS 0:2020 – Proof of Age Standards Scheme – General Requirements and Definitions

PASS 1:2020 – Proof of Age Standards Scheme – Requirements for Identity and Age Verification

PASS 2:2020 – Proof of Age Standards Scheme – Requirements for e-ID Validation Technology

PASS 3:2020 – Proof of Age Standards Scheme – Requirements for Data Protection and Privacy

PASS 4:2020 – Proof of Age Standards Scheme – Requirements for Proof of Age Card Design and Construction.

Other Documents

Scheme Clients will find a substantial amount of supporting materials, guidance, advice and templates to assist with preparing and implementing their data protection systems. This section provides a list of some of the relevant materials that have been used in the preparation of this scheme or may be useful to Scheme Clients.

EDPB – Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679

EA 1/22 A:2016 – EA Procedure and Criteria For the Evaluation of Conformity Assessment Schemes by EA Accreditation Body Member

Accountability Framework, published by the UK Information Commissioner's Office

UK Additional Accreditation Requirements for Certification Bodies

Guidance Notes, including checklists produced and published by the UK Information Commissioner's Office

WP29 – Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679

WP29 – Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

WP29 – Guidelines on Personal data breach notification under Regulation 2016/679

WP29 – Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

WP29 – Guidelines on Data Protection Officers ('DPOs')

WP29 – Guidelines for identifying a controller or processor's lead supervisory authority

WP29 – Guidelines on the right to data portability

WP29 – Guidelines on consent under Regulation 2016/679

WP29 – Guidelines on transparency under Regulation 2016/679

WP29 – Opinion 02/2012 on facial recognition in online and mobile services (WP 192)

United Kingdom's Data Ethics Framework (updated 30th August 2018)

The use of guidance and materials published by the UK Government or the Information Commissioner's Office is under terms of the licence under the Open Government Licence (OGL) v3.0. – http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/









Terms and Definitions



3 Terms and Definitions

In this document:

"shall" indicates a requirement

"should" indicates a recommendation

"may" indicates a permission

"can" indicates a possibility or a capability

GUIDANCE NOTES are shown in italic text and are intended to assist the reader with understanding provisions.

When referring to the ACCS Standards, refer to the ACCS Standard, followed by the year of issue, followed by the provision – such as **ACCS 0:2021, 4.3.**

3.1 Age Appropriate Design Code (AADC)	means the Code of Practice laid before Parliament and issued under s.123 of the Data Protection Act 2018.
3.2 Age Assurance	means the process of gaining a reliable indication of the age of an individual to an appropriate level of confidence.
3.3 Age Attribute	means a piece of information about the age of a natural person.
3.4 Age Attribute Exchange	means an online internet gateway for age check providers and relying parties to assess user asserted, permissioned and verified attributes [PAS 1296:2018 – 2.1.2].
3.5 Age Categorisation	means an indication established that an individual is of an age that is within a category of ages, over a certain age or under a certain age to a specified level of confidence and by reference to information or factors related to that individual.
3.6 Age Check Practice Statement	means the document describing the operational practices and procedures of an age check service [PAS 1296:2018 – 2.1.1].
3.7 Age Check Provider	means an organisation responsible for all the processes with establishing and maintaining a subject's identity attributes [PAS 1296:2018 – 2.1.2].
3.8 Age Check Service	means the entity that makes available attributes for the purposes of age checking [PAS 1296:2018 – 2.1.5].

3.9 Age Determination	means an indication established that an individual has a particular age stated to a specified level of confidence and by reference to information related to that individual [PAS 1296:2018 – 2.1.4].
3.10 Age Estimation	means an indication by estimation that an individual is likely to fall within a category of ages, over a certain age or under a certain age to a specified level of confidence by reference to inherent features or behaviours related to that individual.
3.11 Age Verification Process	means the inter-related or interacting activities that transforms a series of attributes into an age verification product [ISO 17065:2012 – 3.5].
3.12 Age Verification Product	means the result of an age verification process [ISO 17065:2012 – 3.4].
3.13 Certification Requirement	means a specified requirement that is fulfilled by the client as a condition of establishing and maintaining certification [ISO 17065:2012 – 3.7].
3.14 Certification Scheme	means the Age Check Certification Scheme [ISO 17065:2012 – 3.9].
3.15 Client	means an organisation that has applied to the Scheme Conformity Assessment Body, Age Check Certification Services Ltd, for certification or been granted certification that is responsible to ACCS for ensuring that the certification requirements are fulfilled [ISO 17065:2012 – 3.1].
3.16 Consent of the data subject	means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

3.17 Contra-indicator	means pieces of information that either contradict statements about a claimed age attribute or claimed identity or raise some doubt over whether the claims are legitimate or genuine.
3.18 Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data.
3.19 CREST Certified Penetration Tester	means a person certified by CREST (International) Ltd to approve vulnerability scan and penetration testing standards.
3.20 Data Ethics Framework	means the framework published by the UK Government on 30th August 2018 as updated from time-to-time.
3.21 Data processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. [UK GDPR Art. 4]
3.22 Data protection by design and default	means the appropriate technical and organisational measures as required by Article 25 of UK GDPR.
3.23 Data Sharing Code	means the Code of Practice laid before Parliament and issued under s.121 of the Data Protection Act 2018.
3.24 Evaluation	means the combination of the selection and determination functions of conformity assessment activities against the scheme rules [ISO 17065:2012 – 3.3].

3.25 High risk processing	means high risk processing which can include the processing of: • special category data • personal data of vulnerable natural persons, in particular of children • personal aspects evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles • processing involving a large amount of personal data and affecting many data subjects
3.26 ICO	means Information Commissioner's Office.
3.27 Impartiality	means the presence of objectivity [ISO 17065:2012 – 3.13].
3.28 Large organisation	means an organisation with more than 250 employees.
3.29 PASS	means the Proof of Age Standards Scheme operated by the PASSCO Community Interest Company of 37 Stoney Street, Nottingham, England, NG1 1LS.
3.30 Personal data	means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
3.31 Personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3.32 Privacy	means giving an individual the means to control how their data is used and who has access to it, for example having appropriate security measures to prevent inappropriate disclosure or giving individuals control over who their data is shared with.
3.33 Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
3.34 Recipient	means a natural or legal person, public authority, agency or another body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with UK law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
3.35 Relying Party	means an organisation relying on results of an online age check to establish the age-related eligibility of an individual for the purpose of a transaction [PAS 1296:2018 – 2.1.21].
3.36 Scheme Owner	means the Age Check Certification Scheme Ltd [ISO 17065:2012 –3.11].
3.37 Scope of Certification	means the identification of the age check functions for which certification is granted, the applicable scheme and the standard, code or regulations (including their date of publication) to which it is judged that the age check function complies [ISO 17065:2012 – 3.10].
3.38 Small organisation	means an organisation that has less than 250 employees.

3.39 Special category data	means any personal information related to the individual's: • racial or ethnic origin • political opinions • religion or philosophical beliefs • trade union membership • genetic data • health • biometric data for the purpose of a unique identification or authentication of a natural person • sexual life • criminal convictions and offences or related security measures
3.40 Top Management	means a person or group of people who directs and controls an organisation at the highest level.
3.41 UKAS	means United Kingdom Accreditation Service.
3.42 UK GDPR	means General Data Protection Regulation (EU) 2016/679, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (withdrawal) Act 2018 and section 205(4) of the Data Protection Act 2018.





4

Data Protection Management Systems



4. Data Protection Management Systems

Leadership and Oversight of Data Protection Responsibilities

4.1.1 Section 4 of these technical requirements set out how top management of the Scheme Client are responsible for ensuring that appropriate technical and organisational measures are actioned and authorised to ensure and demonstrate that the processing of personal data complies with the principles relating to processing of personal data through effective leadership and oversight.

Note 1: *The measures taken by top management should:*

a) be linked to the scope, context, nature and purposes of the data processing

b) be adapted to the risks of likelihood and severity for the rights and freedoms of natural persons (see section 4.4)

c) be applied to all processing activities within the scope of these technical requirements throughout the lifecycle of the Age Check products, processes or services, starting from ensuring privacy by design and default in the development of products, processes and services involving personal data processing (see section 5.1)

d) ensure that only information that is necessary for the purposes of the processing are processed and are only accessed by designated personnel

e) be consistent with the Age Check Practice Statement, which shall describe the operational practices and procedures of the Age Check Service as required by PAS 1296:2018 – 2.1.1 (see section 4.2)

4.1.2 Top Management shall on a regular basis (as a minimum annually) consider, approve, update and record its consideration of the following matters:

a) the Age Check Practice Statement (see section 4.2)

b) the Data Protection Impact Assessment (see section 4.3), how the data processing necessary for their products, processes and services may affect individuals and justify any adverse impact identified

c) Data Protection Policies (see section 4.3)

d) whether or not the appointment of a designated Data Protection Officer is required and to make such a suitable appointment if required, or if not required to appoint a person with appropriate seniority to have responsibility for data protection (see section 4.5)

e) the effectiveness of communications, training and awareness of the Scheme Client's data protection controls (see section 4.7)

f) the results of any internal or external audits, including audits carried out by the Scheme, to assess the response to identified non-conformity, areas for improvement or proposed preventative measures (see section 4.3.10 - 4.3.13)

g) any personal data breaches and corrective actions taken (see section 4.9)

Note 1: *Data Protection Officers or those exercising data protection responsibilities should not wait for formal reviews to take place before drawing the attention of top management to potential deficiencies in data protection controls or policies.*
The (at least) annual review is intended to provide an opportunity for top management to take a whole organisation look at the operation and effectiveness of its data protection controls and policies; not to deal with individual incidents.

4.1.3 Top Management shall be accountable for decisions made about data protection and privacy as required by Article 5(2) of UK GDPR; shall maintain an open and honest approach to data processing and shall ensure compliance with all transparency obligations.

Note 1: *If Scheme Clients are a larger organisation (over 250 employees) they may choose to put in place a structured privacy management framework. This can help to create a culture of commitment to data protection, by embedding systematic and demonstrable compliance across the organisation. Amongst other things, the framework should include:*

a) robust program controls informed by the requirements of the UK GDPR

b) appropriate reporting structures

c) assessment and evaluation procedures

Note 2: *If Scheme Clients are a smaller organisation they may likely benefit from a smaller scale approach to accountability as set out in Article 5(2) of UK GDPR. Amongst other things they should:*

a) ensure a good level of understanding and awareness of data protection amongst their staff

b) implement comprehensive but proportionate policies and procedures for handling personal data

c) keep records of what they do and why

Note 3: *Controllers and processors each have their own documentation obligations. If the Scheme Client has 250 or more employees, they should document all of their processing activities. There is a limited exemption for small and medium-sized organisations. If they have fewer than 250 employees, they only need to document processing activities that:*

a) are not occasional

b) could result in a risk to the rights and freedoms of individuals

c) involve the processing of special categories of data such as biometric identification data

***Note 4:** Scheme Clients may find the Information Commissioner's Accountability Framework a useful guide for implementing appropriate requirements under this section.*

4.1.4 The Top Management shall be responsible for ensuring that the Scheme Client have determined and documented the lawful basis of processing data for their Age Check process prior to commencing any processing of that data (See Section 5.2). This shall include:

a) identifying an appropriate lawful basis for the processing as set out in Article 6 of UK GDPR, prior to commencing processing that cannot subsequently be changed and connect it to the identified purpose of processing and privacy information provided to individuals when data was collected

b) verifying that the processing is necessary for the purpose for which it was collected, and that there is no other reasonable and less-intrusive way to achieve that purpose

c) if processing special category data, identifying the specific conditions in Article 9 of UK GDPR permitting the processing of that data, noting the requirements of Section 5.9 and the scope exclusions set out in Section 1.7 of these Technical Requirements

d) where processing involves carrying out solely automated individual decision making with legal or similarly significant effects, identifying a specific condition in Article 22 of UK GDPR permitting the processing of that data

e) not undertaking any unlawful data processing activities

***Note 1:** Scheme Clients should note that the processing of data should not result in an infringement of copyright, a breach of an enforceable contractual agreement, a breach of industry-specific legislation or regulations or a breach of the Human Rights Act 1998.*

***Note 2:** Scheme Clients may need to take their own legal advice on other relevant legal requirements. If Scheme Clients have processed personal data unlawfully, the UK GDPR gives individuals the right to erase that data or restrict the processing of it.*

***Note 3:** The requirement that Scheme Clients should process data in a fair way, means that they should handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.*

***Note 4:** Scheme Clients should consider more generally how their data processing affects the interests of the people concerned – as a group and individually, in order to make sure they are processing the personal data fairly. If Scheme Clients have obtained*

and used the information fairly in relation to most of the people it relates to, but unfairly in relation to one individual, that can amount to a breach of the requirements for fair processing of data.

Age Check Practice Statement

Note 1: *The Age Check Practice Statement, as required by PAS 1296:2018, 2.1.1, describes the operational practices and procedures of the Age Check Service, which should be used to help inform the data processing policies and controls that need to be put into place.*

4.2.1 The Scheme Clients that are Age Check Services shall:

a) have a publicly stated commitment to supporting measures of best practice to reduce the access children have to age-restricted goods, content and services

b) act in a manner that is consistent with that commitment

c) co-operate and support other parties in acting in a manner that is consistent with that commitment

4.2.2 The Scheme Clients that are Age Check Services shall develop and adopt an Age Check Practice Statement which shall include as a minimum:

a) a commitment to continual improvement of age checking practices

b) age bands that users are to be checked against and data sources suitable for age checking that age band

c) any legal and regulatory age checking requirements that might apply to the relying party's service

d) whether user anonymity is a significant factor for the relying party's users

e) frequency of age re-checks needed

f) the quality levels required for the accuracy of the age check, including the minimum trust capability categories of any data sources used, given the nature of the online service, its users and regulatory environment

g) a requirement for enhanced data protection techniques, such as data minimisation, pseudonymisation, anonymisation

h) where consent to age check personal data processing might be required and other data protection requirements

i) any known exploits to circumvent age checks with any associated security measures needed to ensure more valid age checks

j) any communication needed about the relying party's age checking policy for regulators, users and the general public

k) the need for awareness of other considerations relevant to the relying party's service and regulatory regime

[PAS 1296:2018 – 3.1]

Data Protection Policies

4.3.1 In addition to the Age Check Practice Statement, Scheme Clients shall establish, document, implement and maintain appropriate data protection policies which state its commitment to deliver products, processes or services involving personal data processing in compliance with UK GDPR and its requirements in relation to accountability. These policies shall include a commitment:

a) to the protection of personal data, including prevention of personal data breaches

b) to implement technical and organisational measures within the organisation to ensure compliance with UK GDPR

4.3.2 Scheme Clients shall establish, implement, maintain and continually improve a set of policies and procedures (Data Protection Management System), which ensure correct implementation and maintenance of personal data related process(es). The data protection management system shall be appropriate to the type, range and volume of products and/or services involving personal data processing and associated risks of likelihood and severity for rights and freedoms of natural persons.

> ***Note 1:*** *Integrating all data protection processes and activities (including reporting mechanisms) into a Data Protection Management System enables the organisation to establish effective governance and continually improve the organisation's data protection. By creating a Data Protection Management System, data protection becomes an integral part of corporate governance.*

4.3.3 The policies in the data protection management system shall contain as a minimum a description of how the Scheme Client:

a) implements safeguards to prevent fraud in relation to the misuse of personal data

b) defines the data protection responsibilities, procedures and processing covered by the scope of the certification (which shall be agreed as part of the Target of Evaluation (see section 1.8 – 1.13)

c) ensures that all relevant components of the processing operations (data, systems, and processes) are covered by the certification (which shall be agreed as part of the Target of Evaluation (see section 1.8 – 1.13)

d) implements safeguards to ensure the integrity, operation, availability and security of data processing systems, including monitoring of evolving privacy and technology issues and updating of the system as required

e) undertakes a data protection impact assessment

f) implements technical and organisational measures to show that they have integrated data protection into their Age Check activities by design and by default

g) assesses whether or not they are obligated to appoint a Data Protection Officer and if they are, to comply with the requirements of Articles 37 – 39 of UK GDPR

h) ensure effective facilitation of data subjects' rights, including policies and procedures on how to handle requests in relation to those rights

i) implements incident management procedures and ensures that personal data breach notification duties are carried out in accordance with the requirements for personal data breach notifications

j) are registered, as appropriate, with the relevant home state information rights regulator, such as the Information Commissioner's Office in the UK

4.3.4 Scheme Clients shall have a procedure to manage documented information, including appropriate:

a) identification, description, review and approval

b) distribution, access, rectification, deletion and use

c) storage and preservation

d) control of changes

e) retention and disposal

Note 1: *Scheme Clients may use an ISO 9001 certified management system in order to manage their Data Protection Management System in an integrated manner, but the specific requirements for the Data Protection Management System set out in this Scheme should still be addressed in that integrated management system.*

4.3.5 Scheme Clients shall maintain a record of processing activity which shall include (as a minimum):

a) the Scheme Client's name and contact details, whether it is a controller or a processor

b) the purposes of the processing

c) a description of the categories of individuals the data relates to and of personal data

d) the categories of recipients of personal data

e) details of transfers to third countries, including a record of the transfer mechanism safeguards in place

f) retention schedules

g) a descriptions of all processing activities carried out by any processors on behalf of the Scheme Client

h) a description of the technical and organisational security measures in place

4.3.6 The record of processing activity shall contain (or include internal links to) the documents covering:

a) information required for privacy notices, such as the lawful basis for the processing and the source of the personal data

b) records of consent

c) controller-processor contracts

d) the location of personal data

e) Data Protection Impact Assessments

f) records of personal data breaches

g) information required for processing special category data under the Data Protection Act 2018 (DPA 2018)

h) retention and erasure policy documents

Note 1: *Scheme Clients may include information about the purposes of the processing, their lawful basis and relevant conditions for processing any special category data publicly available in their privacy notice(s).*

4.3.7 Records shall be legible, maintained in good condition, retrievable and retained for a defined period with consideration given to relevant legal or customer requirements.

4.3.8 Scheme Clients shall implement a Data Retention Policy setting standard retention periods necessary and relevant to the data processing.

4.3.9 The Data Retention Policy:

a) shall not permit indefinite data retention

b) shall remove the need to keep copies or images of originating identification documents for longer than 30 calendar days (as a maximum) unless a specific legal requirement exists to keep them for a longer period

c) may permit for reuse of the age attribute during a future transaction within 12 calendar months

d) may provide for the renewal of a data retention period at each future transaction

e) may provide for de-personalisation or pseudonymisation of the data for future processing beyond the standard retention period

4.3.10 Scheme Clients shall conduct internal audits of their data processing and the implementation of their data protection management system at least annually, covering all requirements of this Scheme to provide Top Management with information on whether:

a) it conforms to the requirements of UK GDPR

b) it conforms to these technical requirements

c) it is effectively implemented and maintained

4.3.11 The scope and frequency of the audits shall take into consideration the risks to personal data processes and activities and previous audit performance.

4.3.12 Scheme Clients shall ensure that internal audits shall be carried out by appropriately trained, competent and impartial auditors.

> ***Note 1:*** *Impartial, in this context, does not necessarily mean external or independent to the Scheme Client, but should encourage auditors that are not directly responsible for the function or process under audit or have not been involved in the design or development of the process under audit.*

4.3.13 Audit reports shall detail any significant deviation from requirements of these technical requirements. In particular, audit reports shall identify issues related to technology or processes which could affect UK GDPR compliance obligations.

Information Security and Risk Management

4.4.1 Scheme Clients shall establish, implement, maintain and continually improve a set of policies and procedures (Information Security Management System), which ensure the confidentiality, integrity and availability of systems and services, including the physical and cyber security of data covering the whole life cycle of the data in the context of the Age Check product, process or service.

Note 1: *Scheme Clients can use an ISO 27001 certified management system in order to manage their data protection management system in an integrated manner, but the specific requirements for the information security, confidentiality, integrity and availability set out in these Technical Requirements shall still be addressed in that integrated management system.*

Note 2: *Scheme Clients may find it useful to refer to the ICO Guidance on Security Outcomes and Guidance issued by the National Cyber Security Centre to build their security resilience.*

4.4.2 Scheme Clients shall ensure they process personal data in a manner that ensures the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using technical or organisational measures based on an assessment of risks.

4.4.3 Scheme Clients shall undertake an analysis of the risks presented by their processing, and use this to assess the level of security they need to put in place. When deciding what measures to implement, they shall take account of the state of the art and costs of implementation.

4.4.4 Scheme Clients shall have in place security measures to ensure that:

a) the data can be accessed, altered, disclosed or deleted only by those that are authorised to do so (and that those people only act within the scope of the authority that was given to them)

b) the data that is held is accurate and complete in relation to why it is being processed; the data remains accessible and usable

c) the data that is held is, where appropriate, unlinked or separated from the data subject, anonymised or pseudonymised to reduce or eliminate the utility of the data to a third party if it is accessed in a security breach

4.4.5 Scheme Clients shall carry out an information security risk assessment as an organisational measure.

4.4.6 When considering security, Scheme Clients shall ensure that the following are addressed:

a) system security – the security of the network and internal information systems, including those which process personal data (including firewalls, access control (including access records), passwords, no shared accounts/passwords, malware, patch management/ software updates, USB use restricted, online security, remote working - secure VPNs, two factor authentication, records of user access)

b) data security – the security of the data that is held within the internal systems, e.g. ensuring appropriate access controls are in place and that data is held securely

c) online security – e.g. the security of external websites and any other online service or application that are used

d) device security – including policies on using Bring-your-own-Devices (BYOD) if this is offered

e) physical security – including covering perimeter security (such as alarms, CCTV, quality doors/locks; access control measures)

f) visitor security (such as sign-in/supervision, ID cards, security passes)

g) IT asset/waste disposal and physical security of physical IT assets including mobile devices

4.4.7 Scheme Clients shall regularly review at least annually their information security policies and measures and, where necessary, improve them, by taking into account technical advancements, new system abilities and functionality, etc. The review shall be documented and approved by the Data Protection Officer or a person of suitable seniority with responsibility for data protection.

4.4.8 Scheme Clients shall be able to restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. Scheme Clients shall document their approach to back-ups, storage of back-ups, implementation and testing of plans in a business continuity plan.

4.4.9 Scheme Clients shall have the ability to intervene into the data processing operation in order to patch or check the system or the process.

4.4.10 Scheme Clients shall use encryption where appropriate, in order to assure that the data is stored and processed securely. The Scheme Client shall implement a policy to describe the use of encryption processes and organisation employees should be educated in such way in order to assure they have assessed the nature and scope of their processing activities and have implemented encryption solution(s) to protect the personal data they store and/or transmit.

> ***Note 1:*** *Scheme Clients should also consider the residual risks that remain, even after they have implemented their encryption solution.*
>
> ***Note 2:*** *There are multiple industry-standard options for encryption, but Scheme Clients may consider using the National Institute of Standards and Technology (NIST) encryptions standards FIPS 140-3, SP 800-175B or SP 800-67.*

4.4.11 Scheme Clients shall undertake Penetration Testing aimed at accessing the specific processing operations of the Age Check product, process or service.

> ***Note 1:*** *Penetration Testing shall be undertaken in accordance with the requirements of Section 6.2.*

Data Protection Officers

4.5.1 A Data Protection Officer shall be appointed to ensure compliance of processes related to personal data protection, if:

a) the Scheme Client is a public authority or body (except for courts acting in their judicial capacity)

b) the Scheme Client's core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking)

c) the Scheme Client's core activities consist of large scale processing of special category data or data relating to criminal convictions and offences

4.5.2 The Data Protection Officer shall be designated on the basis of professional skills, experience and knowledge of data protection law and practices.

4.5.3 The Scheme Client shall ensure that the Data Protection Officer is involved in all issues related to the protection of personal data and shall allocate appropriate budget and resources to fulfil his/her tasks.

4.5.4 The Data Protection Officer shall report to top management.

4.5.5 The Scheme Client shall ensure that the Data Protection Officer can exercise his/her tasks with necessary independence and confidentiality. In case the Data Protection Officer is in charge of other tasks it shall not result in a conflict of interest.

4.5.6 The Data Protection Officer shall have due regard to the risk associated with data processing operations in performing the following tasks:

a) inform and advise the organisation and the employees who carry out personal data processing of their obligations

b) monitor compliance of the organisation with the compliance obligations and internal policies and provisions including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits

c) organise the conduct of periodic reviews of the set of technical and organisational measures related to personal data protection

d) provide advice where requested with regard to the Data Protection Impact Assessment and monitor its performance

e) co-operate with the ICO

f) act as the contact point for the ICO on issues relating to personal data, where appropriate

4.5.7 The organisation shall communicate the contact details of the Data Protection Officer to the ICO and other stakeholders whenever required.

> ***Note 1:*** *The Data Protection Officer can be an employee or a contracted person or shared across organisations. Professional skills and experience shall cover both management skills, IT/IS aspects and knowledge of the organisation's products and services.*
>
> ***Note 2:*** *The Article 29 Guidelines on Data Protection Officers ('DPOs') can be used to identify and mitigate the potential situation of conflict of interest.*
>
> ***Note 3****: Organisations may also appoint data protection specialists for different aspects of their data processing operations.*

Data Protection Impact Assessment (DPIA)

4.6.1 All Scheme Clients shall determine the activities, products and services involving personal data prior to processing considering the life cycle of the data.

4.6.2 Scheme Clients, with the support of any data processors, are required by law to undertake a Data Protection Impact Assessment (as described further in s.4.6.5), but in addition to that all Scheme Clients shall have carried out a Data Protection Impact Assessment for all certified processes prior to the processing commencing.

> ***Note 1:*** *A DPIA is a process to help Scheme Clients identify, assess and minimise the data protection risks of a project or service output. A DPIA should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage.*
>
> ***Note 2:*** *The DPIA can be a single document, or could be a series of assessments with clearly defined scope and applicability to different processing operations. Scheme Clients should take care to ensure that the totality of their DPIA(s) cover the whole of the Target of Evaluation for certification.*

4.6.3 All Scheme Clients shall define a procedure and criteria for conducting a DPIA, including the production of a template for use by staff undertaking assessments. These criteria shall take into account the technological state of the art and the nature, scope, context and purposes of the processing resulting in a high risk to the rights and freedoms of natural persons in accordance with Article 35 of UK GDPR.

4.6.4 To assess the level of risk, Scheme Clients shall identify both the likelihood and the severity of any impact on data subjects. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. Scheme Clients should bear in mind that some data subjects may be less resilient than others and may have additional needs to secure the protection of their data.

4.6.5 A DPIA shall contain as a minimum:

a) a systematic description of the processing operations and the purposes of the processing

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes

c) an assessment of the risks to the rights and freedoms of data subjects

d) the risk category of personal data

e) abnormal conditions and reasonably foreseeable situations that may lead to personal data breaches

f) the measures to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate regulatory compliance taking into account the rights and legitimate interests of data subjects and other persons concerned

g) any change of the risk represented by processing operations, including planned or new developments, and new or modified activities, products and services

4.6.6 Scheme Clients shall have a specific DPIA (in addition to any DPIA required for their overall processing) for any data processing operations that may be high risk as required by Article 35(4) of UK GDPR.

Note 1: *A specific DPIA may not necessarily be in a separate document, but where referring to high risk data processing operations within a generic DPIA, these should be clearly marked and delineated.*

Note 2: *When considering if the processing is likely to result in high risk, organisations should check against the below indicators:*

- *evaluation or scoring*
- *automated decision-making with legal or similar significant effect*
- *systematic monitoring*
- *sensitive data or data of a highly personal nature*
- *data processed on a large scale*
- *matching or combining datasets*
- *data concerning vulnerable data subjects*

- *innovative use or applying new technological or organisational solutions*
- *preventing data subjects from exercising a right or using a service or contract*

4.6.7 Scheme Clients shall regularly review, develop and manage the DPIA through a multi-disciplinary approach that considers any:

a) substantial changes to the nature, scope and context of data processing

b) marketing, commercial or business development

c) operations, information technology and security

d) legal and other relevant functions including views of data subjects or their representatives

If appropriate, particular advice on the content of the DPIA from the Data Protection Officer shall be sought.

4.6.8 The Data Protection Impact Assessment shall be documented.

4.6.9 Scheme Clients shall communicate the outputs of the Data Protection Impact Assessment to the relevant levels and functions of the organisation including the data processors, as appropriate.

4.6.10 In certain circumstances set out in Article 36 of UK GDPR, Scheme Clients shall be required to consult with the Information Commissioner's Office where the DPIA for high risk data processing cannot be mitigated.

4.6.11 Data Protection Impact Assessments should be published, except to the extent that security sensitive information can be redacted.

Training and Awareness for Staff and Contractors

4.7.1 All Scheme Clients shall implement a programme of training and education for all personnel. These measures shall be subject to regular review.

> ***Note 1:*** *Training is dependent on the operational functions of the team member or contractor. It is not necessary for all training to be provided to all staff, but any staff accessing personal data should have at least generic UK GDPR training supplemented by subject or function specific training directly relevant to their roles.*
>
> ***Note 2:*** *All staff should understand basic principles of data protection including how to recognise a request to exercise data subject rights, access to our use of information or when information is being inappropriately disposed of or left unsupervised or uncontrolled.*

Note 3: *Regular review includes a review both of the learning needs of individual team members and of the adequacy, quality and effectiveness of the training provision itself. Reviews of learning needs should be undertaken at least annually and reviews of training provision should be undertaken at least every three years or following any significant changes in UK GDPR legislation or practice.*

4.7.2 The Scheme Client shall provide training to team members or contractors prior to them being permitted unsupervised access to personal data. The training shall be refreshed periodically, which should not be less frequent than annually.

4.7.3 The Scheme Client shall provide training programmes that:

a) incorporate national and sector-specific requirements, including these technical requirements

b) is comprehensive and includes training for all staff on key areas of data protection such as handling requests, data sharing, information security, personal data breaches and records management

c) consider the training needs of all staff and use this information to compile the training programme

d) assign responsibilities for managing information governance and data protection training across the organisation and has training plans or strategies in place to meet training needs within agreed time-scales

e) have dedicated and trained resources available to deliver training to all staff

f) regularly review the programme to ensure that it remains accurate and up to date

g) shall be approved by top management

4.7.4 The Scheme Client shall:

a) conduct an assessment at the end of the training to test staff understanding and make sure that it is effective, which may include a minimum pass mark

b) keep copies of the training material provided on record as well as details of who receives the training

c) monitor training completion in line with organisational requirements at all levels of the organisation, and follow up with staff who do not complete the training

d) ensure that staff are able to provide feedback on the training they receive

4.7.5 The Scheme Client shall:

a) internally communicate information relevant to the data protection management system among the various levels and functions of the organisation, including changes to the management system, as appropriate

b) ensure its communication process(es) enable(s) persons doing work under the organisation's control to contribute to continual improvement

4.7.6 The Data Protection Policies and Age Check Practice Statement shall be available, communicated, understood and applied within the organisation including subcontractors and service suppliers if needed, as well as available to relevant interested parties, as appropriate.

> ***Note 1:*** *There is no requirement to publish the Age Check Practice Statement on a website, although Scheme Clients may choose to do so. It may not be appropriate to make all parts of the Age Check Practice Statement available outside the Scheme Client if it is necessary to protect the organisation from information security threats.*

4.7.7 The Scheme Client shall ensure that any customer-specific policies or requirements, codes of conduct, binding corporate rules etc. are understood, implemented and clearly communicated to relevant staff and, where appropriate, suppliers and service providers.

Sub-Contractors and External Providers Processing Personal Data

4.8.1 All Scheme Clients are responsible for the activities of any sub-contractors or providers where they are processing personal data for or on behalf of the Scheme Client. Scheme Clients shall have contracts in place for subcontractors involved in processing personal data.

> ***Note 1:*** *Contracts should demonstrate security and probity and shall in particular follow stringent diligence processes in accordance with the Technical Requirements in this document.*

4.8.2 The contract shall include a requirement to comply with the relevant aspects of these Technical Requirements relating to data privacy, protection and security, which shall be clearly identified.

4.8.3 Scheme Clients shall ensure that outsourced processes are controlled or influenced in accordance with articles 26 and 28 – 32 of UK GDPR and to ensure the protection of the data subject's rights. The type and extent of control or influence to be applied shall be defined taking into account the nature, scope, context and purposes of the processing resulting in a high risk to the rights and freedoms of natural persons.

In particular:

a) Scheme Clients shall only use external providers providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing shall meet the compliance obligations and ensure the protection of the data subject's rights

b) processing by an external provider shall be governed by a contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the data controller

c) personal data shall only be processed by an external provider if this provider has been given instructions from the controller to do so, or if required to do so by UK law

d) records of processing activities shall be maintained by external providers, containing information such as the name and contact details of the controller, the purposes of the processing, a description of the categories of data subjects and the categories of personal data, and envisaged time limits for erasure of the different categories of data

e) records of all categories of processing activities shall also be kept by an external provider, including information on the categories of processing carried out on behalf of each controller

f) external providers shall cooperate, on request, with the ICO in the performance of its tasks

g) the controller and processor shall take steps to ensure that any external provider who has access to personal data, acting under their authority, shall not process this data unless they have been instructed to do so by the controller or UK law

4.8.4 That contract shall stipulate, in particular, that the external provider:

a) processes the personal data only on documented instructions from the Scheme Client, including with regard to transfers of personal data to a third country or an international organisation

b) ensures that persons authorised to process the personal data have committed themselves to confidentiality

c) takes all specified measures related to personal data security

d) assists the Scheme Client by appropriate technical and organisational measures adapted to the nature of processing

e) assists the Scheme Client in ensuring compliance with the obligations pursuant to articles

32 to 36, taking into account the nature of processing

f) at the choice of the Scheme Client, deletes or returns all the personal data to the organisation after the end of the provision of services relating to processing

g) makes available to the Scheme Client all information necessary to demonstrate compliance with the compliance obligations and contributes to audits, including inspections, conducted by the Scheme Client or another auditor mandated by the Scheme Client, including those appointed by the Scheme

h) shall not engage another processor and/or service provider without prior specific or general written authorisation of the Scheme Client

i) shall notify the Scheme Client without undue delay after becoming aware of a personal data breach and any infringement of UK GDPR

Managing Personal Data Breaches

4.9.1 All Scheme Clients shall establish, implement and maintain the process(es) needed to prepare for and respond to potential personal data breach situations.

4.9.2 The Scheme Client shall:

a) prepare to respond by planning actions to prevent or mitigate personal data breaches and their consequences, appropriately to the magnitude of breaches and their potential impact

b) respond to actual data breach situations

c) periodically test the planned response actions, where practicable

d) periodically review and revise the process(es) and planned response actions, in particular after the occurrence of personal data breach situations or tests

e) provide relevant information and training related to personal data breach preparedness and respond, as appropriate, to relevant interested parties, including persons working under its control

f) ensure that near misses are identified and reported as good practice

g) ensure there is a review of breaches/near misses to improve systems, training and provide opportunities for continuous improvement

4.9.3 Any data processor shall notify the data controller without undue delay after becoming aware of a personal data breach.

4.9.4 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, Scheme Clients shall communicate the personal data breach to the data subject without undue delay.

4.9.5 In addition, in the case of a personal data breach, Scheme Clients shall, within 72 hours, notify the ICO about the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In addition, if the data breach is likely to affect certification under these technical requirements, then the Scheme Client shall also notify the Scheme of the circumstances of the data breach (but shall not disclose any personal data to the Scheme in doing so).

4.9.6 The communication to the data subject and/or to the ICO shall meet requirements expressed in articles 33 and 34 of UK GDPR.

4.9.7 In communications with the data subject and/or the ICO, Scheme Clients shall describe, in clear and plain language, the nature of the personal data breach and, at least:

a) the name and contact details of the Data Protection Officer (if the organisation has one) or other contact points where more information can be obtained

b) a description of the likely consequences of the personal data breach

c) a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including the measures taken to mitigate any possible adverse effects

4.9.8 Scheme Clients shall maintain records of any data breaches comprising the facts relating to the personal data breach, its effects and the remedial action taken. These records shall be made available to the ICO and the Scheme on request.

> ***Note 1:*** *Scheme Clients should ensure that they record all breaches, regardless of whether or not they need to be reported to the ICO.*
>
> ***Note 2:*** *Article 33(5) of UK GDPR requires that Scheme Clients document the facts relating to the breach, its effects and the remedial action taken. This is part of their overall obligation to comply with the accountability principle, and allows the ICO to verify the organisation's compliance with its notification duties under the UK GDPR.*
>
> ***Note 3:*** *As with any security incident, Scheme Clients should investigate whether or not the breach was a result of human error or a system issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.*
>
> ***Note 4:*** *As part of the breach management process Scheme Clients should undertake a risk assessment and have an appropriate risk assessment matrix to help to manage breaches on a day to day basis. This helps to assess the impact of breaches and meet*

the reporting and recording requirements. This also provides a basis for the breach policy and helps to demonstrate the accountability as a data controller.

***Note 5:** As a result of a breach, Scheme Clients may experience a higher volume of data protection requests or complaints, particularly in relation to access requests and erasure. Scheme Clients should have a contingency plan in place to deal with the possibility of this. It is important that Scheme Clients continue to deal with those requests and complaints, alongside any other work that has been generated as a result of the breach. Scheme Clients should also consider how to manage the impact to individuals, including explaining how they may pursue compensation should the situation warrant it.*







5

Requirements for Data Processing



5. Requirements for Data Processing

Data Protection by Design & Default

5.1.1 Scheme Clients shall implement service and product development processes to ensure that data protection is considered from the outset and incorporated into every stage of the service and product design by default.

5.1.2 The plans and records for service and product development and design shall:

a) provide a specific section relating to data protection considerations

b) identify the key risks identified relating to data processing that are identified by the service and product development team

c) provide for the input of the Data Protection Officer (see section 4.5)

d) provide for the input of learning from service and product development iterations, including from stakeholder and staff feedback

e) be kept for a minimum of 12 months following the release of the product or service into a live environment

Lawful Basis of Processing

5.2.1 Scheme Clients shall have a record of which lawful basis of processing they are relying on for each of their processing activities, and justification for choosing that basis. Scheme Clients shall document their lawful basis of processing in a record of processing activities, which shall be consistent with the decisions of top management as required by section 4.1.4. Scheme Clients shall be able to justify that the lawful basis of processing selected is appropriate for the purpose of the processing.

Note 1: *In order to demonstrate this, Scheme Clients could include information about the lawful basis (or bases, if more than one applies) in their privacy notice. Under the transparency provisions of the UK GDPR, Scheme Clients need to give people information (see section 5.8) about:*

- *their intended purposes for processing the personal data*
- *the lawful basis for the processing*

Note 2: *In case special categories of data are processed, Scheme Clients should document both their lawful basis for processing and their special category condition so that they can demonstrate compliance and accountability.*

Fairness

5.2.2 Scheme Clients shall consider and document their consideration of how the processing may affect the individuals concerned and justify any adverse impact.

5.2.3 Scheme Clients shall not deceive or mislead individuals (collectively or individually) when they collect and process personal data. A statement made, action taken or material omission during the data collection process shall be treated as misleading if:

a) it is not true

b) its overall presentation is in any way likely to deceive individuals even if the information is factually correct

c) it omits or hides material information

d) it is presented in a manner that is unclear, unintelligible, ambiguous or untimely

e) it results in actions or behaviours that the individual would not reasonably expect

Note 1: *The record of consideration of the fairness of data collection and processing may be included in the Data Protection Impact Assessment (see Section 4.6).*

Consent

5.2.4 Where the processing is based on the legal basis of consent, the Scheme Clients shall:

a) have checked and documented that consent is the most appropriate lawful basis for processing

b) have made the request for consent prominent and separate from their terms and conditions, provided privacy information to ensure that consent is fully informed

c) have asked people to positively opt in

d) have not used pre-ticked boxes or any other type of default consent

e) have used clear, plain language that is easy to understand

f) have specified why the data is necessary and what it shall be processed for

g) have given separate distinct ('granular') options to consent separately to different purposes and types of processing

h) have provided the name of their organisation and any third party controllers who shall be relying on the consent

i) provide a means for individuals to withdraw their consent without detriment

j) avoid making consent a precondition of a service

5.2.5 Scheme Clients shall ensure that individuals can refuse to consent without detriment.

5.2.6 If Scheme Clients offer online services directly to children, they should only seek consent if they have age-verification measures (and parental-consent measures for younger children) in place. When relying on the consent of children, Scheme Clients shall provide information (in an age appropriate manner) to ensure that the child understands what they are consenting to, and they do not exploit any imbalance of power in the relationship between them and the children.

5.2.7 When offering online services to children on the basis of consent, Scheme Clients shall ensure that anyone who provides their own consent is at least 13 years old. When offering online services to children on the basis of consent, organisations must obtain parental consent to the processing for children who are under the age of 13, and make reasonable efforts to verify that the person providing consent holds parental responsibility for the child.

5.2.8 Scheme Clients shall keep a record of when and how they got consent from the individual and also keep a record of exactly what they were told at the time.

5.2.9 Scheme Clients shall have in place measures to regularly review consents to check that the relationship, the processing and the purposes have not changed.

> ***Note 1:*** *Scheme Clients should have processes in place to refresh consent at appropriate intervals, including any parental consents. They should consider using privacy dashboards or other preference-management tools as a matter of good practice.*

5.2.10 Scheme Clients shall make it clear and easy for individuals to withdraw their consent at any time, and publicise how to do so and act on withdrawals of consent as soon as they can and should never penalise individuals who wish to withdraw consent.

> ***Note 1:*** *Consent is not required for the discharge of a legal obligation to carry out age verification, but if a person's personal data is retained after the legal obligation has been discharged (i.e. for customer accounts or re-verification) consent may be the most appropriate lawful basis and shall be obtained before continuing to process the personal data.*

Contract

5.2.11 Where the processing is based on the legal basis of contract, the Scheme Clients shall:

a) identify a contract with the individual and demonstrate how they need to process their personal data to comply with their obligations under the contract

b) identify why it is necessary for the performance of the contract to process the personal data

c) identify circumstances where a contract is not yet executed, but the individual has asked for something as a first step (e.g. verify their age) and it is necessary to process their personal data to do what they ask. This applies even if they do not actually go on to

enter into a contract (for instance because they are not old enough to access the goods, content or services), as long as the processing was in the context of a potential contract with that individual

d) provide guidance and information to individuals that are subject to contract on how they can exercise their data rights

Note 1: *Scheme Clients could discharge the requirements under 5.2.11 (a) by:*

a) maintaining a template contracts database

b) recording the personal data obligations generated by the template contracts

c) maintaining a record of contract review

Legal Obligation

5.2.12 Where the processing is based on the legal basis of discharge of a legal obligation, the Scheme Clients shall:

a) have identified the specific legal obligation(s) and maintained a documented schedule of the obligation(s) relied upon

b) identify why it is necessary for the discharge of the legal obligation to process the personal data

c) have identified different requirements (such as differing age verification laws) in different jurisdictions and recorded this in the documented schedule of the obligation(s) relied upon.

5.2.13 Scheme Clients shall have assessed the limitations of when their legal obligation has been discharged and another lawful basis of processing may be required from that point forward. As an example, the legal obligation to age verify only applies up until the point that the age verification process is completed. Processing personal data after that point would require a different lawful basis.

5.2.14 Scheme Clients shall provide guidance and information to individuals where their data is being processed in discharge of a legal obligation on how they can exercise their data rights.

Note 1: *Scheme Clients should note that the legal obligation to comply with age restrictions on goods, content or services is principally placed upon the seller of those goods, content or services. However, many pieces of age restriction legislation can transfer (or more accurately duplicate) that legal obligation on to a third party upon whom the seller of the age restricted goods, content or services relies (known as the relying party) and whose act or default resulted in the commission of an offence.*

Note 2: *Where Scheme Clients are acting for relying parties in the discharge of their legal obligations, this should be carefully recorded in the contract with the relying party. Care should be given to understanding whether or not the Scheme Client is discharging a legal or contractual obligation as its intended lawful basis of processing the data – which may differ from service to service or product to product.*

Note 3: *The Scheme Client should be able to identify the obligation(s) in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, the Scheme Client can refer to a government website or to industry guidance that explains generally applicable legal obligations.*

Vital Interests

5.2.15 Scheme Clients shall not rely upon the vital interests of the data subject for the processing being certified as a lawful basis of processing.

Note 1: *Scheme Clients may want to consider the vital interests of data subjects when planning for the potential need to share data in an emergency (see section 5.11.5).*

Public Tasks

5.2.16 The only circumstances under this Scheme whereby Scheme Clients that are Age Check Services may rely on the discharge of a public function for their data processing is when their processing is necessary for the purposes of:

a) age assessments under s.55 of the Borders, Citizenship and Immigration Act 2009

b) age assessments under s.51 of the Modern Slavery Act 2015

5.2.17 Scheme Clients shall undertake such age assessments in accordance with the Home Office Assessing Age Code of Practice V3.0. Scheme Clients shall be able to demonstrate that they have an active role with a competent public authority in undertaking age assessments.

Legitimate Interests

5.2.18 Where the processing is based on the legal basis of legitimate interests, the Scheme Clients shall:

a) have assessed the specific and relevant legitimate interest(s) and maintained a documented schedule of the legitimate interests(s) relied upon

b) ensure that policies regarding the responsibility to protect an individual's interests are applied, including undertaking a balancing assessment to demonstrate that the individual's interests do not override the legitimate interest(s) relied upon

c) have verified that the processing is necessary to discharge those legitimate interest(s) and there is no less intrusive way to achieve the same result

d) have identified different requirements (such as differing age verification laws) in different jurisdictions and recorded this in the documented schedule of the legitimate interest(s) relied upon

5.2.19 A Legitimate Interests Assessment shall be carried out, including undertaking an assessment of:

a) the purpose test (identify the legitimate interest)

b) the necessity test (consider if the processing is necessary)

c) the balancing test (consider the individual's interests)

Note 1: *In undertaking a balancing assessment, Scheme Clients may utilise the Information Commissioner's Template for Legitimate Interests Assessments.*

5.2.20 Scheme Clients shall provide guidance and information to individuals (See Section 5.8 – Privacy Policy) where their data is being processed in discharge of a legitimate interest(s) on how they can exercise their data rights.

5.2.21 Scheme Clients shall not rely on legitimate interests as a lawful basis of processing where the interests of the data controller or third party are overridden by the legitimate interests and fundamental rights of the data subject, particularly where the data subject is a child.

Note 1: *Scheme Clients should tell people in the privacy information that they are relying on legitimate interests, and explain what these interests are.*

Note 2: *If Scheme Clients want to process the personal data for a new purpose, Scheme Clients may be able to continue processing under legitimate interests as long as their new purpose is compatible with the original purpose.*

Note 3: *If Scheme Clients rely on legitimate interests, the right to data portability does not apply (See section 5.7.21 - 5.7.24).*

Purpose Limitation

5.3.1 Scheme Clients shall have clearly identified and documented the purpose or purposes for processing data prior to processing, which shall only process data in a manner consistent with the decisions of top management on purpose.

5.3.2 The purpose or purposes for data processing shall be publicly available in the Scheme Client's privacy information for individuals.

5.3.3 Scheme Clients shall regularly review their processing and, where necessary, update their record of processing activities (See Section 4.3.5) and their privacy information for individuals (See Section 5.8). The regular reviews shall be documented.

5.3.4 If a Scheme Client plans to use personal data for a new purpose other than a legal obligation or function set out in law, they shall have a process in place to ensure that this is compatible with their original purpose or they shall get specific consent for the new purpose.

> ***Note 1:*** *Scheme Clients should specify the purpose or purposes for processing personal data within the documentation they are required to keep as part of the records of processing activities, as well as to specify their purposes in the privacy information for individuals.*
>
> ***Note 2:*** *If the Scheme Client is a small organisation (employing fewer than 250 staff) and it is exempt from some documentation requirements, it may not need to formally document all of the purposes to comply with the purpose limitation principle.*

Data Minimisation

5.4.1 Scheme Clients shall only collect and process personal data that is adequate, relevant and necessary for the purposes for which they are processed.

5.4.2 Scheme Clients shall collect sufficient personal data to properly fulfil those purposes. The data is only collected in identifiable form to the extent strictly necessary in relation to the purpose for which it is collected. This applies to the amount of personal data collected, to the extent of their data processing and the period of storage and accessibility.

5.4.3 Scheme Clients shall take action to eliminate, in particular:

a) unnecessary creation of temporary files

b) unnecessary log in information

c) unnecessary unfiltered data (such as data captured in ID scanning processes)

d) unnecessary data retention (see below)

e) unnecessary augmentation of data sets to show or potentially indicate user behaviours, personal preferences, interests, location or movements

5.4.4 Scheme Clients shall periodically review the data they hold, and delete anything that is not needed.

5.4.5 Scheme Clients shall identify and document the data retention periods in a retention schedule, including justification of their retention policy by reference to the period of time that the Scheme Client needs the data for their specified purposes (see section 4.3.8 – 4.3.9).

5.4.6 Scheme Clients that use personal data for the training of or processing data using artificial intelligence or machine learning technologies shall establish and document a data minimisation policy and implement effective controls in connection with the accuracy, handling, storage and use of training data for that purpose. This is in addition to the requirement at s.4.2.2 (g) regarding the Scheme Client's data minimisation approach in the Age Check Practice Statement.

> ***Note 1:*** *Scheme Clients should identify the minimum amount of personal data they need to fulfil their purpose and should hold that much information, but no more. In order to assess whether Scheme Clients are holding the right amount of personal data, they should first be clear about why they need it. Scheme Clients should periodically review the processing to check that the personal data they hold is still relevant and adequate for their purposes, and delete anything they no longer need. This is closely linked with the storage limitation principle.*
>
> ***Note 2:*** *Augmentation of data can occur when two or more seemingly independent sets of data contain a common data field or can be temporally aligned. This can result in the ability to identify user behaviour, personal preferences, interests, location or movements, even if the second data set does not include personally identifiable information. As an example, a transaction code applied to a data packet or cookie on an adult entertainment site with an electronic time stamp, but containing no personally identifiable information, could be augmented with a second data set showing identity and age verification records and an electronic time stamp. The two together could be utilised to identify the user of a particular adult entertainment site (which may in turn give an indication of sexual preference or orientation) and compromise the privacy and security of that individual's personal data.*
>
> ***Note 3:*** *The ICO have issued guidance on artificial intelligence and data protection.*

Accuracy

5.5.1 Scheme Clients shall ensure that any personal data created by their processing is accurate and kept up to date.

5.5.2 Scheme Clients shall check the accuracy of the data they collect, and record the source of that data. There shall be a process in place to identify when they need to keep the data updated to properly fulfil their purpose, and to update it as necessary.

5.5.3 Scheme Clients shall clearly identify any matters of opinion, including artificial intelligence analysis of claimed age attributes or biometric or inherent features and, where appropriate, record who (or which version of an algorithm has reached that opinion) and any relevant changes that occur to the underlying facts. The documentation supporting the handling of outputs of artificial intelligence systems shall state that results shall not be interpreted as statements of fact, but as statistically informed guesses.

5.5.4 Scheme Clients shall ensure that any personal data identified as being inaccurate are erased or rectified without delay and notify anybody that the personal data has been shared with.

5.5.5 Scheme Clients shall have detection mechanisms in place during the authentication and identification processes to identify contra-indicators to claimed age attributes. The detection mechanism should be able to recognise that the discovery of a contra-indicator does not necessarily mean that a claim is not legitimate. The Scheme Client's process(es) should trigger mitigation actions when a contra-indicator is detected.

> ***Note 1:*** *The processes put in place to identify contra-indicators should not result in increased surveillance of data subjects.*
>
> ***Note 2:*** *Contra-indicators are pieces of information that either contradict statements about a claimed age attribute or claimed identity or raise some doubt over whether the claims are legitimate or genuine. They may include:*
>
> a) *inconsistencies between printed data on an identity document and check digits or data captured through near field communication (NFC) chips*
>
> b) *multiple use of the age attribute in contradictory circumstances (such as use to prove that a holder is under a certain age, perhaps for a concessionary fare, but also over the same age, perhaps to access an age restricted cinema viewing)*
>
> c) *two identification documents presented by the same person, but with differences on the face of the documents, such as name, address, gender, date of birth, etc.*

5.5.6 The Scheme Client's processes should react to contra-indicators discovered after initial identification or authentication in the same manner as if they occurred during initial identification or authentication. The processes should result in an evaluation of whether an age attribute record needs to be reviewed to determine if it should cease to assert a claimed age based on the contra-indicator(s) discovered.

5.5.7 Scheme Clients shall ensure that their processing systems are designed in a manner which fosters the principle of accuracy, including functionalities that ensure that data that is identified as inaccurate may be erased or rectified without delay.

5.5.8 Scheme Clients shall keep a record of any challenges to the accuracy of personal data and where they acknowledge a mistake, that personal data shall be clearly identified as a mistake.

5.5.9 Where appropriate, Scheme Clients shall provide user documentation to relying parties with all relevant guidance about actions to be taken by the relying party in order to comply with accuracy requirements.

Note 1: *In practice, this means that Scheme Clients should:*

a) take reasonable steps to ensure the accuracy of any personal data

b) ensure that the source and status of personal data is clear

c) carefully consider any challenges to the accuracy of information

d) consider whether it is necessary to periodically update the information

Note 2: *There is often confusion about whether it is appropriate to keep records of things that happened which should not have happened. Individuals understandably do not want their records to be tarnished by inaccurate records. However, Scheme Clients may legitimately need their records to accurately reflect the order of events. Keeping a record of the mistake and its correction might also be in the individual's best interests. It is acceptable to keep records of mistakes, provided those records are not misleading about the facts. Scheme Clients may need to add a note to make it clear that a mistake was made.*

Note 3: *It may be impractical to check the accuracy of personal data someone else provides. In order to ensure that the records are not inaccurate or misleading in this case, Scheme Clients should:*

a) accurately record the information provided

b) accurately record the source of the information

c) take reasonable steps in the circumstances to ensure the accuracy of the information

d) carefully consider any challenges to the accuracy of the information

Note 4: *Individuals have the absolute right to have incorrect personal data rectified. Individuals do not have the right to erasure just because data is inaccurate. However, the accuracy principle requires Scheme Clients to take all reasonable steps to erase or rectify inaccurate data without delay, and it may be reasonable to erase the data in some cases. If an individual asks for deletion of the inaccurate data it is therefore good practice to consider this request (See section 5.7.11 - 5.7.13).*

Storage Limitation

5.6.1 Scheme Clients shall maintain a record of the types of personal data held and the purpose that it is held. This shall include documented justification for how long the personal data is kept.

5.6.2 Scheme Clients shall ensure that any personal data is held in accordance with documented storage retention policies (See Section 4.3.8 – 4.3.9).

5.6.3 Scheme Clients shall ensure that their processing systems are designed in a manner which fosters the principle of storage limitation, including functionalities that ensure that data is automatically erased, regularly weeded, permanently deleted or anonymised in accordance with the documented storage retention policies.

> ***Note 1:*** *Scheme Clients should provide deletion tools perhaps setting an automated deletion schedule (such as deletion after 30 days), instant deletion (such as once the purpose has been discharged, the data is instantly deleted) or self-serve deletion (such as by the data subject, ad hoc requests or record correction/duplication).*

5.6.4 Scheme Clients shall ensure that their systems provide for the ability to intervene in the processing operations in order to guarantee data subject rights and allow corrections, erasures or restrictions on the data.

5.6.5 Scheme Clients shall ensure that they anonymise any personal data kept for public interest archiving, scientific or historical research, or statistical purposes. They shall also need to have in place a storage retention policy or schedule for such data.

> ***Note 1:*** *Scheme Clients should note that it is not necessary to retain any records of individual age attributes, primary credentials or any personal data for the purposes of subsequent audit of compliance with these Scheme Rules. For relying parties, age check services and age exchange services depending upon the adopted process, it is not likely to be necessary for the Scheme to access personal data for certification monitoring.*

> ***Note 2:*** *Scheme Clients should not keep the data for longer than they actually need it. Ensuring that Scheme Clients erase or anonymise personal data when they no longer need it reduces the risk that it becomes irrelevant, excessive, inaccurate or out of date and also reduces the risk that they use such data in error – to the detriment of all concerned. Retention policies or retention schedules list the types of record or information Scheme Clients hold, what they use it for, and how long they intend to keep it.*

> ***Note 3:*** *Scheme Clients should consider their stated purposes for processing the personal data. They can keep it as long as one of those purposes still applies, but they should not keep data indefinitely 'just in case', or if there is only a small possibility that they shall use it. Future audits, where a sampling process is undertaken, should not be considered a suitable reason for retaining the whole data set. Sampling should be temporally aligned with the earliest opportunity that the sample can be reviewed and checked. Once checked, the sample should be returned to the data set and managed in accordance with the applicable data retention policy.*

> ***Note 4:*** *Scheme Clients should also consider whether they need to keep a record of a relationship with the individual once that relationship ends. They may not need to delete all personal data when the relationship ends. They may need to keep some information*

so that they can confirm that the relationship existed – and that it has ended – as well as some of its details. In the context of age verification, it is unlikely that it would be necessary to retain a record of the relationship with the age verified party once that relationship has ended.

Note 5: *When no longer needed, Scheme Clients can either erase (delete) or anonymise the data.*

Note 6: *Scheme Clients should remember that there is a significant difference between permanently deleting personal data and taking it offline. If personal data is stored offline, this should reduce its availability and the risk of misuse or mistake. However, they are still processing personal data. Scheme Clients should only store it offline (rather than delete it) if they can still justify holding it. Scheme Clients should be prepared to respond to subject access requests for personal data stored offline, and they should still comply with all the other principles and rights.*

Note 7: *Scheme Clients that utilise immutable ledgers (such as Blockchain) in order to store personal data, should develop methods for the ledger to be hashed or the cryptographic key to be such as to render the data stored in the chain to be irretrievable or anonymised once it becomes due for deletion. The process of maintaining the integrity of the immutable ledger should provide for privacy by design and the exercise of data subject rights.*

Data Subject Rights

5.7.1 All Scheme Clients shall ensure that data subject rights are respected.

5.7.2 Where possible, Scheme Clients shall provide online tools to enable data subjects to exercise their rights through 'self-service' options or, where self-service is not possible, through simplified online privacy management tools.

5.7.3 Scheme Clients shall ensure that applicable exemptions to Data Subject Rights are correctly applied. The applicable exemptions are set out in Schedules 2,3 and 4 of the Data Protection Act 2018 or if a request is 'manifestly excessive or repetitive'. Further information about the applicable exemptions can be found in ICO Guidance.

5.7.4 Scheme Clients shall ensure that they notify any third parties if any rectification or erasure of personal data or restriction of processing has been carried out in accordance with Articles 16, 17(1) and 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

Right to Be Informed (Privacy Policy)

5.7.5 Scheme Clients shall ensure that a Privacy Policy is produced and published on their website or app (in accordance with the requirements of Section 5.8 – Transparency), which shall contain (as a minimum):

a) the name and contact details of the Scheme Client

b) the name and contact details of any Data Protection representative in the United Kingdom used by the Scheme Client (if applicable - see section 1.15)

c) the contact details of the Data Protection Officer (if applicable)

d) the purposes of the processing

e) the lawful basis for the processing

f) the legitimate interests for the processing (if applicable)

g) the categories of personal data obtained (if the personal data is not obtained from the individual it relates to)

h) the recipients or categories of recipients of the personal data

i) the details of transfers of the personal data to any third countries or international organisations (if applicable)

j) the retention periods for the personal data

k) the rights available to individuals in respect of the processing

l) the right to withdraw consent (if applicable)

m) the right to lodge a complaint with the ICO

n) the source of the personal data (if the personal data is not obtained from the individual it relates to)

o) the details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to), including reference to specific age restrictions or control legislation where this is appropriate

p) the details of the existence of automated decision-making, including profiling or use of age estimation artificial intelligence (if applicable) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

5.7.6 In addition to publishing their Privacy Policy on their website, Scheme Clients shall provide a link to it or a copy of it or provide a 'just-in-time' notice providing enough information at the point of collection with the ability to find out more from the full Privacy Policy:

a) at the time they start to collect their personal data from an individual

b) if an individual seeks to exercise their data rights

c) if an individual makes a complaint about the Scheme Client

5.7.7 If a Scheme Client operates an age check service that is conducted on behalf of a client but without the direct knowledge of the individual (a 'stealth check'), the Scheme Client shall ensure that:

a) their client's website contains a warning to purchasers of age restricted goods that an age checking process would be undertaken and the identity of the organisation undertaking that process, with a link to the Scheme Client's Privacy Notice

b) within a reasonable period (and no later than one month) of obtaining the personal data to carry out the age checking process, notify the individual of the Scheme Client's identity and provide a link to or copy of their Privacy Policy. This action can be undertaken by the Scheme Client or by their client

Note 1: *Scheme Clients should provide individuals with the necessary information in an easily accessible form. This applies equally if Scheme Clients collect personal data from the individual it relates to or if they obtain personal data from another source.*

Note 2: *Scheme Clients may meet this requirement by putting the information on their website (this is often how organisations deliver privacy information), however they should proactively make individuals aware of this information and they need to give them an easy way to access it. Simply putting it on the website, in case people happen to look there, is not enough.*

Note 3: *Scheme Clients could undertake an information audit to find out what personal data they hold and what they do with it. In preparing privacy information, Scheme Clients should put themselves in the position of the people they are collecting information about and they should carry out user testing to evaluate how effective their privacy information is.*

The Right of Access

5.7.8 Scheme Clients shall ensure that they recognise, understand and address subject access requests. This shall include how verbal subject access requests are identified, recorded and addressed.

5.7.9 Scheme Clients shall respond to subject access requests within one calendar month, unless there is a lawful exemption to responding, which shall be explained to the data subject. If it is not possible to respond within one month, they shall contact the individual within one month and explain the permitted circumstances applicable to extend the time limit to respond to the request.

Note 1: *The permitted circumstances are if the request is complex or Scheme Clients have received a number of requests from the individual, in which case, the time to respond can be extended by a further two months provided the Scheme Client has notified the data subject within one calendar month that an extension is being applied.*

Note 2: *The lawful exemptions to responding to a subject access request are set out in Schedules 2,3 and 4 of the Data Protection Act 2018 or if a request is 'manifestly excessive or repetitive'. Further information about the applicable exemptions can be found in ICO Guidance.*

5.7.10 Scheme Clients shall explain a refusal to issue an age attribute token indicating that an individual is over 18, when the Scheme Client has determined that they are not and, therefore, the subject access request is received from a person that the Scheme Client believes may be a child. In such circumstances, the response shall be in clear and plain language appropriate to be understood by a child.

Note 1: *Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them. A common enquiry from a person with parental responsibly may be seeking to find out why their child has been granted access to an age restricted product, content or service.*

Note 2: *Before responding to a subject access request for information held about a child, Scheme Clients should consider whether the child is mature enough to understand their rights. If Scheme Clients are confident that the child can understand their rights, then they should usually respond directly to the child. They may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.*

Note 3: *What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, Scheme Clients should take into account, among other things:*

a) the child's level of maturity and their ability to make decisions like this

b) the nature of the personal data

c) any court orders relating to parental access or responsibility that may apply

d) any duty of confidence owed to the child or young person

e) any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment

f) any detriment to the child or young person if individuals with parental responsibility cannot access this information

g) any views the child or young person has on whether their parents should have access to information about them

The Right to Rectification

5.7.11 Scheme Clients shall ensure that they recognise, understand and address a request for rectification of allegedly inaccurate data. This shall include how verbal requests are identified, recorded and addressed.

5.7.12 Scheme Clients shall respond to the request for rectification within one calendar month. If it is not possible to respond within one month, they shall contact the individual within one month and explain the permitted circumstances applicable to extend the time limit to respond to the request.

Note 1: *The permitted circumstances are if the request is complex or Scheme Clients have received a number of requests from the individual, in which case, the time to respond can be extended by a further two months provided the Scheme Client has notified the data subject within one calendar month that an extension is being applied.*

5.7.13 Scheme Clients shall notify any relying party of any rectification of inaccurate data that could reasonably have caused that relying party to make a transactional decision that was improper (i.e. they refused a sale of an age restricted item on the mistaken notification from the Scheme Client that the individual was under age).

Note 1: *Scheme Clients should comply with a request for rectification without undue delay and at the latest within one month of receipt of the request or (if later) within one month of receipt of:*

a) any information requested to confirm the requester's identity

b) a fee (only in certain circumstances). In most cases, Scheme Clients cannot charge a fee to comply with a request for rectification. However, Scheme Clients can charge a "reasonable fee" for the administrative costs of complying with the request if it is manifestly unfounded or excessive. Scheme Clients should base the reasonable fee on the administrative costs of complying with the request

Note 2: *Scheme Clients should calculate the time limit from the day they receive the request (whether it is a working day or not) until the corresponding calendar date in the next month.*

The Right to Erasure

5.7.14 Scheme Clients shall ensure that they recognise, understand and address a request for erasure of personal data. This shall include how verbal requests are identified, recorded and addressed.

5.7.15 Scheme Clients shall respond to the request for erasure of personal data within one calendar month. If it is not possible to respond within one month, they shall contact the individual within one month and explain the permitted circumstances applicable to extend the time limit to respond to the request.

> ***Note 1:*** *The permitted circumstances are if the request is complex or Scheme Clients have received a number of requests from the individual, in which case, the time to respond can be extended by a further two months provided the Scheme Client has notified the data subject within one calendar month that an extension is being applied.*

5.7.16 Scheme Clients shall explain to the individual the consequences of the erasure of personal data including any diminished utility that the individual may experience (such as having to repeat age verification processes in the future).

> ***Note 1:*** *Scheme Clients should prepare for requests for erasure by doing the following:*
>
> a) *recognising a request for erasure and understand when the right applies*
>
> b) *having a policy for how to record requests that are received verbally*
>
> c) *understanding when to refuse a request*
>
> d) *being aware of the information that is needed to provide to individuals when they do so*
>
> ***Note 2:*** *Complying with requests for erasure means that Scheme Clients should also consider the following:*
>
> a) *have processes in place to ensure that the response to a request for erasure is without undue delay and within one month of receipt*
>
> b) *be aware of the circumstances when they can extend the time limit to respond to a request*
>
> c) *understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children*
>
> d) *have procedures in place to inform any recipients if they erase any data they have shared with them*
>
> e) *have appropriate methods in place to erase information*

The Right to Restrict Processing

5.7.17 Scheme Clients shall ensure that they recognise, understand and address a request to restrict processing of personal data. This shall include how verbal requests are identified, recorded and addressed.

5.7.18 Scheme Clients shall restrict processing of an individual's data where:

a) the individual contests the accuracy of their personal data and the Scheme Client is verifying the accuracy of the data

b) the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the UK GDPR) and the individual opposes erasure and requests restriction instead

c) the personal data is no longer needed but the individual needs the Scheme Client to keep it in order to establish, exercise or defend a legal claim

d) the individual has objected to the processing of their data under Article 21(1), and the Scheme Client is considering whether their legitimate grounds for processing override those of the individual

5.7.19 Scheme Clients shall respond to the request to restrict the processing of personal data within one calendar month. If it is not possible to respond within one month, they shall contact the individual within one month and explain the permitted circumstances applicable to extend the time limit to respond to the request.

Note 1: *The permitted circumstances are if the request is complex or Scheme Clients have received a number of requests from the individual, in which case, the time to respond can be extended by a further two months provided the Scheme Client has notified the data subject within one calendar month that an extension is being applied.*

5.7.20 Scheme Clients shall explain to data subjects the consequences of restrictions on the processing of personal data, including any diminished utility that the individual may experience (such as having to repeat age verification processes in the future).

Note 1: *Scheme Clients can prepare for requests for restriction by assuring the below:*

a) know how to recognise a request for restriction and how to understand when the right applies

b) have a policy in place for how to record requests they receive verbally

c) understand when they can refuse a request and are aware of the information they need to provide to individuals when they do so

Note 2: *In complying with requests for restriction of processing, Scheme Clients should:*

a) have processes in place to ensure that they respond to a request for restriction without undue delay and within one month of receipt

b) be aware of the circumstances when they can extend the time limit to respond to a request

c) have appropriate methods in place to restrict the processing of personal data on their systems

d) have appropriate methods in place to indicate on their systems that further processing has been restricted

e) understand the circumstances when they can process personal data that has been restricted

f) have procedures in place to inform any recipients if they restrict any data they have shared with their users

g) understand that they need to tell individuals before they lift a restriction on processing

The Right to Data Portability

5.7.21 Scheme Clients shall ensure that they recognise, understand and address a request for data portability. This shall include how verbal requests are identified, recorded and addressed.

Note 1: *Data subjects have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:*

a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1)

b) the processing is carried out by automated means

5.7.22 Where a request for data portability is to be refused, Scheme Clients shall communicate the reasons for that decision to the data subject.

5.7.23 Scheme Clients shall respond to the request for data portability within one calendar month. If it is not possible to respond within one month, they shall contact the individual within one month and explain the permitted circumstances applicable to extend the time limit to respond to the request.

Note 1: *The permitted circumstances are if the request is complex or Scheme Clients have received a number of requests from the individual, in which case, the time to respond can be extended by a further two months provided the Scheme Client has notified the data subject within one calendar month that an extension is being applied.*

5.7.24 Scheme Clients can comply with data portability by subscribing to or engaging with a relevant trade association interoperability framework or Age Check Exchange. This framework or Age Check Exchange shall be certified in accordance with PAS 1296:2018.

Note 1: *The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.*

Note 2: *The right to data portability entitles an individual to:*

- *receive a copy of their personal data and*
- *have their personal data transmitted from one controller to another controller*

Note 3: *Individuals have the right to receive their personal data and store it for further personal use. This allows the individual to manage and reuse their personal data. For example, an individual wants to retrieve their contact list from a webmail application to build a wedding list or to store their data in a personal data store.*

Note 4: *Scheme Clients can achieve this by either:*

a) directly transmitting the requested data to the individual or

b) providing access to an automated tool that allows the individual to extract the requested data themselves.

Note 5: *This does not create an obligation for Scheme Clients to allow individuals more general and routine access to their systems – only for the extraction of their data following a portability request. In addition, it does not require Scheme Clients to provide users with access to cryptographic keys or other hash data to access immutable ledgers.*

Note 6: *Scheme Clients may have a preferred method of providing the information requested depending on the amount and complexity of the data requested. In either case, Scheme Clients need to ensure that the method is secure.*

The Right to Object

5.7.25 Scheme Clients shall ensure that they recognise, understand and address an objection to data processing. This shall include how verbal requests are identified, recorded and addressed.

5.7.26 Scheme Clients shall respond to the objection to data processing within one calendar month. If it is not possible to respond within one month, they shall contact the individual within one month and explain the permitted circumstances applicable to extend the time limit to respond to the request.

> ***Note 1:*** *The permitted circumstances are if the request is complex or Scheme Clients have received a number of requests from the individual, in which case, the time to respond can be extended by a further two months provided the Scheme Client has notified the data subject within one calendar month that an extension is being applied.*

5.7.27 Scheme Clients shall explain the consequences of objecting to data processing to the data subject, including any diminished utility that the individual may experience (such as having to repeat age verification processes in the future).

5.7.28 Scheme Clients should note that individuals have an absolute right to stop their data being used for direct marketing. The processing of personal data for the purposes of direct marketing is not in scope for this Scheme.

> ***Note 1:*** *Individuals cannot object if the processing is necessary for:*
>
> *a) a task carried out in the public interest*
>
> *b) the exercise of official authority vested in the Scheme Client*
>
> *c) the Scheme Client's legitimate interests (or those of a third party)*
>
> ***Note 2:*** *Where Scheme Clients have received an objection to the processing of personal data and they have no grounds to refuse, Scheme Clients should stop or not begin processing the data.*
>
> ***Note 3:*** *This may mean that Scheme Clients should erase personal data as the definition of processing under the UK GDPR is broad, and includes storing data. However, as noted above, this may not always be the most appropriate action to take.*

Rights in Relation to Automated Decision Making and Profiling

5.7.29 Scheme Clients shall have identified if the processing being certified engages automated decision making or profiling. This shall either be:

a) automated individual decision-making (making a decision solely by automated means without any human involvement) or

b) profiling (automated processing of personal data to evaluate certain things about an individual)

Note 1: *Profiling can be part of an automated decision-making process.*

5.7.30 Scheme Clients providing an age checking service or age assurance within the context of an information society service and that determines if an individual is likely to be over or under a defined age or between an age range by reference to biometric or inherent features, shall identify and record if it is an automated decision-making process even if, by default, a negative result requires human intervention to carry out alternate age verification processes.

Note 1: *Some of the methods companies may wish to consider for age verification:*

a) ***self-declaration –*** *This is where a user simply states their age but does not provide any evidence to confirm it. It may be suitable for low risk processing or when used in conjunction with other techniques*

b) ***artificial intelligence –*** *It may be possible to make an estimate of a user's age by using artificial intelligence to analyse the way in which the user interacts with a company's service. Similarly, the company could use this type of profiling to check that the way a user interacts with their service is consistent with their self-declared age. This technique typically provides a greater level of certainty about the age of users with increased use of the service*

c) ***third party age verification services –*** *Scheme Clients may choose to use a third party service to provide an assurance of the age of the users (where they are not the age verification service themselves). Such services typically work on an 'attribute' system where they request confirmation of a particular user attribute (in this case age or age range) and the service provides them with a 'yes' or 'no' answer. This method reduces the amount of personal data clients need to collect and may allow them to take advantage of technological expertise and latest developments in the field*

d) ***account holder confirmation –*** *Scheme Clients may be able to rely upon confirmation of user age from an existing account holder who they know to be an adult. For example, if they provide a logged-in or subscription based service, they may allow the main (confirmed adult) account holder to set up child profiles, restrict further access with a password or PIN, or simply confirm the age range of additional account users*

e) ***technical measures –*** *Technical measures which discourage false declarations of age, or identify and close under age accounts, may be useful to support or strengthen self-declaration mechanisms. Examples include neutral presentation of age declaration screens (rather than nudging towards the selection of certain ages), or preventing users from immediately resubmitting a new age if they are denied access to the service when they first self-declare their age*

f) ***hard identifiers –*** *Scheme Clients can confirm age using solutions which link back to formal identity documents or 'hard identifiers' such as a passport*

5.7.31 Scheme Clients shall not carry out profiling of performance at work, economic situation, health, personal preferences, interests, reliability, location or movements. This includes the augmentation of data with other data that may, when taken collectively, create a profile of any of these features of an individual. This would include, for instance, databases that may show information about an individual's browsing habits or interests connected to age restricted goods, content or services.

5.7.32 Scheme Clients that are Age Check Services shall not carry out profiling of personal data for marketing purposes. Scheme Clients that are Information Society Services may only carry out profiling of personal data for marketing purposes in accordance with the requirements of ACCS 3, s. 5.12.

5.7.33 Scheme Clients shall act transparently, with publicly available information about the algorithms used, automated or semi-automated decision making, retention and uses of data; for automated decision-making and profiling.

> ***Note 1:*** *Such information does not have to reveal proprietary or commercially confidential information, but should provide sufficient detail to enable an average individual to understand how their data is processed in the automated decision-making and profiling. The published information may contain information about the statistical accuracy of the automated decision-making and profiling when tested.*

5.7.34 Scheme Clients shall test any age estimation systems to secure mitigation of inherent bias on grounds of race, sex or disability. Such variances caused by inherent bias shall not be such as to establish prohibited conduct under Part 2 of the Equalities Act 2010 and shall be accompanied by an Equalities Impact Assessment (even if one is not required by the Public Sector Equalities Duty under the Equalities Act 2010).

5.7.35 Scheme Clients shall publish an automated decision-making and profiling ethics statement, which shall include reference, where appropriate, to the United Kingdom's Data Ethics Framework.

> ***Note 1:*** *Scheme Clients should:*
>
> a) *provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual*
>
> b) *use appropriate mathematical or statistical procedures*
>
> c) *ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it*

d) put appropriate technical and organisational measures in place, so that they can correct inaccuracies and minimise the risk of errors

e) secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects

5.7.36 Scheme Clients shall provide for data subjects to exercise their rights in relation to automated decision making and profiling, including:

a) the right to request human intervention

b) the right to express their point of view

c) the right to contest the decision

5.7.37 Scheme Clients shall not make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them unless:

a) it is necessary for the performance of a contract between child and data controller, and the controller has put in place suitable measures to safeguard the child's rights, freedoms and legitimate interests

b) it is authorised by UK law which includes suitable measures to safeguard the child's rights, freedoms and legitimate interests

c) it is based on the child's explicit consent, and the controller has put in place suitable measures to safeguard the child's rights, freedoms and legitimate interests

Transparency

5.8.1 Scheme Clients shall make the current version of their Privacy Policy publicly available through a website or app, but should also keep previous versions of the policy that would have been applicable at the time that current personal data held by the Scheme Client was initially collected.

5.8.2 Scheme Clients shall ensure that by default individuals are told why, when, where and how their personal data is being processed, and by which organisations (including ensuring a UK-based representative is appointed and notified to the individual).

5.8.3 Where an age check service is processing the personal data of children, in addition to the above including gaining the consent of the data subject, the Scheme Client should (for children aged 13 – 18) or shall (for children aged under 13):

a) publish a clear and comprehensive online Privacy Policy describing their information practices for personal information collected online from children

b) provide direct notice to parents or lawful guardians and obtain verifiable parental/lawful guardian consent, before collecting personal information online from children (parental consent is only required under Article 8 of UK GDPR if the lawful basis of processing being relied upon is consent (Article 6 (1)(a))

c) give parents/lawful guardians the choice of consenting to the operator's collection and internal use of a child's information, but prohibit the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this shall be made clear to parents)

d) provide parents/lawful guardians with access to their child's personal information to review and/or have the information deleted

e) give parents/lawful guardians the opportunity to prevent further use or online collection of a child's personal information

f) maintain the confidentiality, security and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security

g) retain personal information collected online from a child for only as long as is necessary to fulfil the purpose for which it was collected, and delete the information using reasonable measures to protect against its unauthorised access or use

5.8.4 Scheme Clients should ensure that they tell individuals about their processing in a way that is easily accessible and easy to understand. Scheme Clients shall use clear and plain language.

Note 1: *Transparency is important, but especially in situations where individuals have a choice about whether they wish to enter into a relationship with the Scheme Clients. If individuals know at the outset what the Scheme Clients shall use their information for, they shall be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship.*

Note 2: *Transparency is important even when Scheme Clients have no direct relationship with the individual and collect their personal data from another source. In some cases, it can be even more important - as individuals may have no idea what the data is collected and used for, and this affects their ability to assert their rights over their data. This is sometimes known as 'invisible processing'.*

Special Category Data and Biometrics

5.9.1 Scheme Clients shall only process biometric data where used as a means of unique identification of an individual in accordance with the requirements for handling special category data.

5.9.2 Scheme Clients shall implement specific safeguards for the processing of special category data including:

a) documenting the types of biometric information used, including whether or not it is used for identification purposes

b) undertaking a specific Data Protection Impact Assessment on the use of special category data which may be accompanied by an Appropriate Policy Document relating to the specific conditions in Schedule 1 of the Data Protection Act 2018

c) providing information about the handling of biometric information in their Privacy Policy

Note 1: *Facial imaging and fingerprint data are just two examples of biometric data used as a means of unique identification of an individual, but these are not exhaustive. Many other types of physical, physiological or behavioural 'fingerprinting' fall within the definition.*

Examples of physical or physiological biometric identification techniques include:

- *facial recognition*
- *fingerprint verification*
- *iris scanning*
- *retinal analysis*
- *voice recognition*
- *ear shape recognition*

Examples of behavioural biometric identification techniques include:

- *keystroke analysis*
- *handwritten signature analysis*
- *gait analysis*
- *gaze analysis (eye tracking)*

Note 2: *Scheme Clients that process digital photographs of individuals should note that this is not automatically biometric data even if used for identification purposes. Although a digital image may allow for identification using physical characteristics, it only becomes biometric data if subject to "specific technical processing". Usually this involves using the image data to create an individual digital template or profile, which in turn is used for automated image matching and identification.*

Note 3: *All biometric data is personal data, as it allows or confirms the identification of an individual. Biometric data is also special category data whenever it is processed "for the purpose of uniquely identifying a natural person". This means that biometric data will be special category data in the vast majority of cases. If biometrics are used to learn something about an individual (such as their age), authenticate their identity, control their access, make a decision about them, or treat them differently in any way, it is likely to be considered processing of special category data.*

International Transfers

5.10.1 Scheme Clients may transfer personal data to a third country or an international organisation only if the transfer is compliant with one of the provisions expressed in articles 44, 45 and 46 of UK GDPR or as permitted by UK data protection legislation.

5.10.2 A Scheme Client contemplating an international transfer of data shall:

a) determine if it is a restricted transfer of data, taking into account the requirements imposed by the United Kingdom leaving the European Union

b) determine if the transfer is covered by adequacy regulations

c) determine if the transfer is covered by appropriate safeguards

d) determine if the transfer is covered by an exception set out in article 49 of UK GDPR

e) undertake a transfer impact assessment to ensure data will continue to have essentially equivalent level of protection as in the UK

Note 1: *Adequacy regulations could be applicable for data transferring out of the UK if the UK Secretary of State has made such regulations under s.17A of the Data Protection Act 2018 or for data transferring into the UK if the source country (or an international organisation such as the EU) has made a reciprocal adequacy decision under the data protection laws applicable in that third country or international organisation.*

Note 2: *An appropriate safeguard could include standard contractual clauses (SCCs) prescribed in Regulations under s.17C of the Data Protection Act 2018 or, for important reasons of public interest in accordance with Regulations under s.18 of the Data Protection Act 2018. Scheme Clients should refer to the latest ICO Guidance on the current list of appropriate safeguards.*

5.10.3 Scheme Clients shall keep a record of any international transfers of personal data that take place.

5.10.4 A Scheme Client shall identify data acquired from anywhere outside the UK before 31st December 2020 (known as 'legacy data' and held under the 'frozen GDPR' provisions in place before the United Kingdom exited the European Union).

Note 1: *'Frozen GDPR' is important protection for data obtained from anywhere overseas under the terms of EU GDPR and held by UK organisations. The Frozen GDPR does not apply to any personal data about individuals who are located in the UK.*

5.10.5 A Scheme Client that is in the UK who offers goods or services to individuals in the EU, or monitors the behaviour of individuals in the EU, shall appoint a suitable representative in the EEA.

Note 1: *A Scheme Client that offers goods or services, such as an age verification service, to a business established in the EU, is not required to appoint a local suitable representative unless it intends to monitor the ongoing behaviour of individuals in the EU (however, Scheme Clients should note that by virtue of s. 5.7.31 and 5.7.32 of these technical requirements, the monitoring of behaviour of individuals for most purposes is prohibited).*

Data Sharing

5.11.1 Scheme Clients may share personal data in a fair and proportionate way in accordance with UK GDPR.

Note 1: *Nothing in these technical requirements place any obligation on Scheme Clients to share their personal data, however, Scheme Clients may be placed under certain lawful obligations by third parties (particularly law enforcement authorities) to do so and, where this occurs, Scheme Clients should exercise appropriate verification of those obligations and due diligence on the identity, process, security and technical organisational measures in place to facilitate that data sharing activity.*

Note 2: *In making decisions about sharing personal data, Scheme Clients may find the ICO's Data Sharing Code and checklist useful.*

5.11.2 Scheme Clients shall include their plans for data sharing, or the circumstances in which it will consider data sharing, in their Data Protection Impact Assessment (see Section 4.6).

5.11.3 Scheme Clients shall record the parameters of their data sharing with third parties in a Data Sharing Agreement. This shall include:

a) carrying out a Data Protection Impact Assessment (see Section 4.6) specifically in relation to the proposed sharing (except in situations where Section 5.11.5 applies)

b) documenting the data to be shared, including the nature of the data records, the start and end date of the data records

c) the providence of the data (such as the Vectors of Trust or Levels of Assurance associated with data – see ACCS 4 – Technical Requirements for Age Check Providers and PAS 1296 for more information about this)

d) the due diligence undertaken on the recipient of the data, including any controls or restrictions placed upon the recipient for use of the data

5.11.4 Scheme Clients shall identify and record the lawful basis of data sharing before sharing any personal information (this is different to the lawful basis of collecting data for processing).

> ***Note 1:*** *The lawful basis for data sharing may not be the same as the lawful basis that the Scheme Client relied upon in the first place when collecting that data.*
> *As an example, the Scheme Client may have relied upon a contract when collecting the data, but during the lifetime of holding the data, the Scheme Client became aware of something affecting the vital interests (life or death) of the individual and decides, proactively, to share that data with a third party, such as the police.*

5.11.5 Scheme Clients shall plan for the potential need to share data in an emergency where it is necessary and proportionate to do so.

> ***Note 1:*** *There is no need for a data sharing agreement to be in place where an emergency situation occurs.*
>
> ***Note 2:*** *An emergency situation includes:*
>
> - *preventing serious physical harm to a person*
> - *preventing loss of human life*
> - *protection of public health*
> - *safeguarding vulnerable adults or children*
> - *responding to an emergency*
> - *an immediate need to protect national security*

5.11.6 Where Scheme Clients undertake sharing of the personal data of children they shall do so with the best interests of the child as a primary consideration.

> ***Note 1:*** *ACCS 3:2021 – Technical Requirements for Age Appropriate Design for Information Society Services has more detail about considerations of the best interests of the child.*

5.11.7 Scheme Clients shall record requests for data sharing together with the decision on whether or not to permit the data sharing and the reasons for reaching the conclusion that the Scheme Client has reached.









6

Technical Evaluation (Method of Evaluation)



6. Test Protocols (Method of Evaluation)

6.1.1 The Conformity Assessment Body for this Scheme shall establish the technical test protocols, including reference to the UK GDPR implications for the system under test (the Target of Evaluation, ToE).

6.1.2 The Conformity Assessment body for this Scheme shall undertake technical evaluation of the age verification system as appropriate. The Technical Evaluation can include any of the following activities, or any other relevant activities for the system submitted for evaluation:

a) **Bona Fide Test Crew Presentation –** Utilising a test crew for bona fide presentation to age verification systems. This can include for false/accurate accept rates, skin tone analysis, gender, age grouping and disfigurement etc

b) **Presentation Attack Detection –** Assessing PAD for human-likeness (but not liveness analysis) and also for identity assets presentation (both genuine and false identity assets). Utilising different presentation attack instruments, PAI species, and PAI series. Testing for 2D and 3D presentation objects. This is sometimes more commonly known as anti-spoofing testing

c) **Detection Device Analysis –** Assess performance on multiple forms of detection devices – webcams, tablets, cameras, mobile telephones – different operating systems (such as Android, iOS, etc.) and at different presentation intensity, distance and angles. Testing device integrated equipment, such as gaming machines or till systems, subject to them being made available to the CAB at the testing studio

d) **Ambient and Directed Lighting Analysis –** Assessing system capabilities under different types of ambient light, either presented at the presentation object or at the detection device. This includes for different light levels from supermarket-style overhead LED lighting, to pub-style sodium lighting, to casino-style multi coloured lighting, to strobe lighting and anything in between. This includes the capability for internal and outdoor lighting. The lighting can be directed ambient to the presentation object (i.e. the person being age estimated) or the detection device (i.e. the camera) or both

e) **Electronic Identity Document Validation Technologies –** Testing system capabilities on identifying ID documents (such as Passports, Driving Licences or other official ID Cards), being able to extract relevant data from those documents (such as through Machine Readable Zones (MRZ) or Near Field Communication (NFC)) and present that data accurately to enable effective Age Determination

f) **Social Proofing –** Assessing the analysis, with a user's consent, of their digital footprint and the related social graphs, which can be interrogated to determine the veracity of a self-asserted identity. This is the ability of systems to gain proof of age through analysis of the social contacts an individual has and asking those social contacts to verify or confirm the age attributes of an individual

g) **Parental Consent –** Assessing the process of identifying and verifying a digital parent or capable guardian related to or responsible for an individual and gaining verification of the age group of the individual through information provided by that parent or capable guardian

h) **Biometric Subject Behaviours –** Assessing systems deployed for identifying and analysing subject behaviours (such as squeezing together one's fingers in hand geometry and a biometric presentation in response to a directive cue, which are both voluntary reactions)

i) **In Situ Testing –** Testing deployed units in real world scenarios. Typically, this comes after the initial certification and is part of the certification monitoring that is put in place to make sure that systems continue to perform as expected

j) **Skin Tone Analysis –** Testing whether or not biometric systems are susceptible to skin tone bias (based on the Fitzpatrick Scale)

Penetration Testing

6.2.1 Scheme Clients shall establish a method of evaluation for vulnerability scanning and penetration testing of age check systems.

6.2.2 Penetration testing shall be undertaken by a CREST Certified Penetration Tester. The vulnerability scanning and penetration testing shall include the following activities (where relevant), or any other relevant activities for the system submitted for evaluation:

a) the requirements for external vulnerability assessment and any file upload capabilities

b) the requirements for server build assessment

c) the requirements for firewall build assessment

d) the requirements for database settings, storage and archiving assessment

e) the requirements for web applications testing

f) the requirements for other platform applications testing

g) the requirements for application programming interface (API) testing, including calls and parameters per call









© Age Check Certification Scheme

Visit us on social media...

@AgeCheckCert





Internationally recognised standards

Our scheme provides evidence that identity and age check practices meet international standards.



Highly qualified certification officers

Our locally trained certification officers are highly qualified professionals in each jurisdiction.



Evidence you can use to demonstrate compliance

Our certificates of conformity are internationally recognised by law enforcement.



Guaranteed independence & impartiality

Our independent board, impartiality committee and ISO processes guarantee impartial certification.

Age Check Certification Scheme

www.accscheme.com

An independent not-for-profit company registered in England and Wales (11493870) at Unit 321B Broadstone Mill, Broadstone Road, Stockport, SK5 7DL

ISBN 978-1-7398513-2-3

0 638266 208948