Proof of Age
Standards Scheme

PAS

PAS 3:2020

Requirements for Data Protection, Privacy and Security

Introduction

The Proof of Age Standards Scheme ("PASS") is the United Kingdom's national Proof of Age Accreditation Scheme, endorsed by the Home Office, the National Police Chiefs' Council (NPCC), the Security Industry Authority (SIA) and law enforcement officers, such as Trading Standards.

The PASS Scheme is operated by a Community Interest Company providing accreditation to suppliers of Proof of Age Cards in the UK.

The Accredited Providers are assessed against the standards set out in:

- PASS 0 – General Principles and Definitions
- PASS 1 – Requirements for Identity and Age Verification
- PASS 2 – Requirements for e-ID Validation Technology
- PASS 3 – Requirements for Data Protection, Privacy and Security
- PASS 4 – Requirements for Proof of Age Card Design and Construction

The PASS Scheme may decide to add further standards for specific types of proof of age services, which shall result in extensions to this list.

All Accredited Providers are required to comply with PASS 0:2020 and any relevant PASS Standards applicable to their business operations. The relevant PASS Standards will be shown on the individual licence agreement between PASSCo CIC and the Accredited Provider.

All Accredited Providers are required to comply with the latest version of the PASS Standards (indicated by the year of issue), subject to any transitional arrangements agreed by the PASS Standards Committee.

The PASS Standards are assessed by qualified, competent auditors appointed by PASS to ensure that Accredited Providers reach and continue to operate to the requirements of the PASS Standards. This means that providers of age restricted goods, content and services can be confident in accepting cards with a PASS hologram, safe in the knowledge that the scheme is supported by the police, Trading Standards and a wide range of trade bodies.

Contents

1. Scope

The Proof of Age Standards Scheme (PASS) Standards are applicable to any Proof of Age Card provider that wishes to operate under the PASS Scheme and have access to use of the PASS registered Trade mark.

This part of the PASS Standards:

- establishes the requirements for Accredited Providers to have clear data protection policies and a principle of privacy by design in their systems;
- sets the parameters for the lawful basis of processing by Accredited Providers under the PASS Scheme;
- addresses processing activities, data minimisation, accuracy, storage, integrity and security of personal data processed by or on behalf of Accredited Providers;
- sets requirements for securing the rights of data subjects;
- identifies the risk mitigation and risk management factors relevant to data processing by Accredited Providers.

The suite of PASS Standards are applied as applicable to the activities of Accredited Providers or Applicant Providers. This will be dependent on the scope of operations of the providers and the services that they provide for citizens.

2. Normative References

Legal Provisions

General Data Protection Regulation (EU) 2016/679;

Data Protection Act 2018;

Borders, Citizenship and Immigration Act 2009;

Modern Slavery Act 2015;

Electronic Identification, Authentication and Trust Services Regulation (EU) 2014/910.

National and International Standards

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

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 9001:2015, Quality management systems – Requirements.

Other Documents

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

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 PASS Standards, refer to the PASS Standard, followed by the year of issue, followed by the provision – such as **PASS 0, 4.3.2**.

The terms and definitions established in PASS 0 apply to this standard and all PASS Standards.

4. Data Protection – General Principles

Data Protection Policies

4.1 The Data Protection Policies of an Accredited Provider shall contain as a minimum a description of how the Accredited Provider:

(a) maintains the privacy of individuals;
(b) implements safeguards to prevent fraud or misuse of personal data;
(c) defines the data protection responsibilities, procedures and processing covered by its processing of data for the purposes of PASS;
(d) ensures that all relevant components of the processing operations (data, systems, and processes) are covered by the policies;
(e) the identification of the lawful basis of processing the personal data for specified purposes;
(f) implements safeguards to ensure the integrity, operation, availability and security of data processing systems, including the monitoring of evolving privacy and technology issues and the updating of the system as required;
(g) undertakes a data protection impact assessment, and implements technical and organisational measures to show that they have integrated data protection into their age check activities;
(h) 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 GDPR;
(i) implements incident management procedures and ensures that personal data breach notification duties are carried out in due time and scope;
(j) are registered, as appropriate, with the relevant home state information rights regulator, such as the Information Commissioner's Office in the UK; and
(k) have appropriate regard for differing data protection regimes in member states.

Privacy by Design

4.2 All PASS Systems operated by or on behalf of Accredited Providers shall:

(a) be designed with data protection in mind, ensuring that users' privacy is protected by default, following the principles of privacy by design;
(b) be subject to legitimate commercial confidentiality, act transparently with publicly available information about the algorithms used, automated or semi-automated decision making, retention and uses of data;

(c) identify and record the lawful basis for processing of users' data at each stage of the age verification process and during the whole life cycle of the Scheme Member's handling of the data including the deletion and or anonymisation;
(d) ensure that individuals are told why, when, where and how their personal data is being processed, and by which organisations (including ensuring an EU-based representative is appointed and notified to the individual);
(e) address the portability of data, the circumstances under which data is to be portable and the criteria for receiving organisations;
(f) ensure that biometric data is handled in accordance with special category personal data;
(g) minimise the processing of personal data necessary to achieve the intended outcome of confirming age; issuing a Proof of Age Card or age attribute as appropriate to the Accredited Provider's lawful activities; additional personal data should not be collected, irrespective of whether it is subsequently securely deleted;
(h) secure the unlinking or separation of the data from the data subject, anonymisation or pseudonymisation or isolation of data systems to minimise risks to data subjects;
(i) process personal data securely in light of the associated risks presented by the processing, including having contractually committed requirements for data processors or subcontractors and the right to intervene to protect the rights and freedoms of citizens and secure patches and system checks to maintain ongoing operational performance;
(j) access the balance of risks of handling personal data with the rights and freedoms of citizens, by utilising a recognised risk assessment methodology, such as the Data Protection Impact Assessment;
(k) facilitate individual's rights (including the rights of access, erasure and rectification);
(l) ensure that personal data is not retained for longer than is necessary to achieve the purposes for which it was originally collected;
(m) provide proof of contractual requirements between the client and any data processors or controllers acting in the chain of custody of personal data relevant to the client's activity;
(n) keep records of processing activities in accordance with Article 30 of GDPR;
(o) map and record data flows, purpose, lawful basis of processing, retention periods and who is responsible for managing specific information assets.

4.3 The data processing of an Accredited Provider shall be assessed by reference to conformity against an approved GDPR Certification Scheme under Article 42 of GDPR.

4.4 The assessment of data processing shall incorporate:

a) The lawful basis for processing
b) The purpose limitation
c) Data minimisation
d) Accuracy of data
e) Storage and Retention of data
f) The rights of data subjects
g) Transparency, including the publication of privacy policies
h) International Transfers of data

About PASS

The PASS Scheme is operated by a Community Interest Company providing accreditation to suppliers of Proof of Age Cards in the United Kingdom. The Accredited Providers are assessed against strict standards by qualified auditors to ensure that they operate to the highest standards. Sellers of age restricted products can be confident in accepting cards with a PASS hologram, safe in the knowledge that the Scheme is supported by the police, Trading Standards and a wide range of trade bodies.

Assurance

Every card that carries a PASS hologram will have been issued by a provider who has been through a stringent application and accreditation process.

Confidence

Production of a PASS hologrammed card at the point of sale affords retailers and their staff the confidence of knowing that the card is a trusted and secure form of identification.

Reliability

The unique PASS hologram is a registered Trade mark, making it a criminal offence to manufacture cards that have a mark similar to the PASS one.

Support

Possession of a PASS accredited card demonstrates that your age and personal details have been verified by your Accredited Provider and you are who you say you are!

PASS

PASSCo C.I.C.

www.pass-scheme.org.uk

A community interest company registered in England at 37 Stoney Street, Nottingham, England, NG1 1LS with the registered number 04570623.