Privacy Policy MyCheckr | Anonymous Age Estimation

MyCheckr does not require or use:

- Any personal details such as name, address, or date of birth

  The estimation is performed completely anonymously.

- No data or images are stored on the device
- After the estimation has completed, any information that was used is entirely deleted
- MyCheckr operates completely offline which negates any risk of any potential interception of information by an external party

MyCheckr process
All processing steps performed locally on the hardware.

- Face is detected (using face detection algorithm)
- Landmarking algorithm is applied (highlights key locations on a person's face)
- Face quality is evaluated (subject pose, face size, image sharpness, spoof attempt) to decide whether to proceed
- If quality criteria are met, the landmark position are passed to the estimation algorithm
- The algorithm processes the data and returns an estimate for the age
- All images and landmark positions are deleted

MyCheckr and GDPR

- The MyCheckr products use our biometrics technology to anonymously estimate age
- Understanding how our technology fits with the GDPR principles of transparency is key to allaying fears and unease about how data is managed during the Age Estimation process
- The latest opinion from the ICO (Information Commissioner's Office) on Age Assurance for the Childrens Code
(14th October 2021) states explicitly sanctions the use of biometric data for higher-risk use-cases to complete age assurance processes under the public interest reason for processing data

This allows the anonymous processing of faces without explicit content – in the environment of restricting access of Children to age restricted goods and services.

The anonymous age estimation technology was independently audited for GDPR compliance. In March 2022 the technology was granted ACCS 2:2021 Technical Requirements for Data Protection and Privacy, the criteria being 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.

The foundation of this certification is on compliance of the processing steps in the technology with UK GDPR, some of which is outlined in the following sections. The certification can be downloaded here

Definitions of biometrics in GDPR

Definition of biometric data in Article 4(14) of the UK GDPR:

Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Definition of special category data in Article 9 of the UK GDPR:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Recital 51 of the UK GDPR further says that:

The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

In the [Commissioner's [the ICO's] Opinion on Age Assurance for the Children's Code](#), first published on 14 October 2021, the ICO states that age estimation "may" involve the processing of biometric data (at para 2.3.2) and then clarifies later at para 4.2.1 that it is only biometric data if it is used to uniquely identify an individual.

The ICO has helpfully clarified that processing biometric data for the purposes of the Age Appropriate Design Code can be lawfully done to meet the 'substantial public interest' exception in the UK GDPR (Article 9(2)(g)).