GDPR: What CRB Cunninghams' (CRBC) consider when processing biometric data (Facial recognition)

What is biometric data?

The GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person".

Facial recognition is one of the "special categories of personal data" that can only be processed if:

- The data subject has given explicit consent;
- Processing is necessary for the purposes of carrying out the obligations and exercising
- specific rights of the controller or of the data subject;
- Processing is necessary to protect the vital interests of the data subject;
- Processing is necessary for the establishment and exercise of defence of legal claims; or
- Processing is necessary for reasons of business interest.

The GDPR states that data processors must implement appropriate "technical and organisational measures" to keep data secure. CRB Cunninghams' complies fully with this requirement. This is part of CRBC's risk-based approach of the UK GDPR.

Privacy impact assessments are mandatory in the case of automated processing, large-scale processing, or when data controllers systematically monitor a publicly accessible area on a large scale, and this will be carried out by the company before any data is uploaded. data controllers will identify the risks the processing presents to data subjects and implement measures tailored to mitigate those risks. A robust DPIA requires diversity of input, and so consulting with data subjects is a critical part of evaluating the fairness and proportionality of the processing.

CRBC's GDPR-compliant facial recognition system will:

- only be used where necessary, proportionate, and legitimate,
- operate based on processing that is fair, lawful & transparent,
- use accurate, adequate, and only relevant data for the minimum amount of time necessary
- to fulfil the purpose of processing,
- be secure against unauthorised tampering, accidental degradation, exposure, or exfiltration,
- support the exercise of data subject rights
- It can be evidenced that using the technology will not generate gender or racial bias

Operators are trained to understand the risks associated with use of the software and understand they are accountable.

This is in addition to the existing UK GDPR rules and regulations that CBRC strictly abide by and follow.