GDPR Compliance of iProov Services

An iProov Position Paper

V2.7 08th February 2023

1. Introduction

On 25th May 2018 the General Data Protection Regulation (GDPR) came into force in Europe, including the United Kingdom. It determines how data is processed within the EEA for any person, regardless of their nationality, and how data of any EEA resident citizen is processed, regardless of where the processing takes place. Compliance with GDPR is a core requirement of iProov's services, and this paper addresses how this compliance is achieved.

This document is commercial, and is not to be taken as binding on, or as containing anything that represents a commitment on the part of iProov Limited ("iProov", "we" or "us").

2. Summary

- iProov acts as a Data Processor on behalf of its client, the Data Controller, or as a Data sub-Processor on behalf of its partner, a Data Processor. It processes data only under the instructions of the data controller and complies with the Core Principles of the GDPR. iProov has appointed its own Data Protection Officer to comply with the requirements of Article 37 of the GDPR.
- Many of the provisions of the GDPR, including its very application, the basis for processing Special Category personal data, and the rights of data subjects are significantly different for processing in the public interest or for public security.
- Data Controllers must judge whether, in processing face imagery for the purposes of ID matching or authentication, Special Category personal data is being processed. This would require explicit user consent. User consent is also a means to comply with the GDPR rules on automated decision-making.
- Other personal data, such as device data and movement data, is processed as well. iProov considers this legitimate as being necessary to prevent fraud.
- Core Principles of security, integrity and confidentiality are supported by iProov's ISO 27001 certification and its use of pseudonymisation and encryption.
- Personal data, including facial imagery, is stored by iProov, as necessary for the purposes for which user consent is granted or a lawful basis for processing is held, after which it is deleted or anonymised.
- iProov relies on the Data Controllers to ensure a lawful basis for processing, including securing the necessary user consents, and is granted relief by the GDPR against the consequences of non-compliance by the Data Controller or other Data Processors.
- Since Brexit, a formal decision was made by the EU that recognises the UK's laws and systems for protection of personal data as adequate. This adequacy decision is expected to last until June 2025. The EU commission will begin to work on deciding whether to extend the adequacy decisions for the UK for a period up to a maximum of four years. iProov will continue to actively monitor applicable legislative changes, and continue to mitigate risks. Where required, iProov may also process EU data solely

within the EU. iProov has an EU representative office in the Netherlands.

3. Scope – Commercial Purposes

The data processed by iProov is Personal Data, and Data Controllers may consider that facial imagery of a Data Subject is Special Category data.

iProov takes care to pseudonymise the imagery so that no information is available that might permit iProov, acting alone, to unambiguously identify the person depicted in the images.

Nevertheless, the GDPR provisions may be interpreted to include such pseudonymous imagery in the definition of Special Category data (unless it has been anonymised and hence ceases to be Personal Data).

Any other categories of data that iProov collects are not Special Category data and hence are not subject to the requirements of Article 9 of the GDPR. iProov processes such data, under Article 6b processing is necessary for the performance of a contract.

Anonymisation may subsequently be used to take all stored data out of the scope of the GDPR according to the provisions of Recital 26:

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. ***To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly****. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.* ***The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable****. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.*

iProov considers that anonymisation of the data it processes and stores is accomplished if:

- facial data is rendered unrecognisable by a person or machine aware of the appearance of the relevant natural person, together with the erasure of any relationship to a pseudonym that could be used (in combination with other data) to identify that natural person.

- Any chain of data that, taken together, might permit a data subject to be identified is irrevocably broken at any point by permanent erasure of linking data.

4. Scope – Public Interest Purposes

Processing of personal data for purposes in the public interest or for the purposes of public security is subject to significantly different requirements. Each public body must review its own legal framework to assess this. Some considerations are:

- Article 2(d) exempts entirely from the provisions of the GDPR processing "*by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*."
- Article 9(g) permits processing of Special Category personal data **without subject consent** provided that "*processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*;"
- Article 22.4 permits automated decision-making based on Special Category personal data under an Article 9(g) provision. Such decision-making may be based on user consent, or alternatively under 22.2(b) **without user consent** if it is "*is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests*;"

In all cases, when acting under a contract with a body that provides data to iProov under a public interest purpose, iProov will use encryption and pseudonymisation to adhere to the core principles and best practice of processing.

5. Compliance with Core Principles

Article 5 outlines the six principles of data processing. These are:

- Lawful, fair and transparent processing
- Purpose Limitation: collected for specified, explicit and legitimate purposes
- Data Minimisation: adequate, relevant and limited
- Accuracy: accurate, kept up to date, erased when inaccurate
- Storage Limitation: stored for no longer than is necessary
- Security, Integrity & Confidentiality: security against unauthorised, unlawful processing or loss, destruction or damage

5.1 iProov relies on the Data Controllers to ensure a lawful basis for processing, including securing the necessary user consents, Lawful, Fair and Transparent Processing

Article 6 states that one of the bases for the lawful processing of personal data is:

*(a) The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes.*

There are demanding requirements in GDPR and in associated guidance notes for obtaining consent to the processing of Personal Data, and alternative bases for lawful processing may be preferred instead. However, Special Category personal data cannot be processed under these bases alone, due to the provisions of Article 9 which require a justification specified in that Article for such processing. Of those GDPR justifications for Special Category processing, only the category of "explicit" consent is applicable. It is the data controller's responsibility to obtain explicit consent for use of the services provided by Iproov as detailed under section 5.2 Purpose Limitation given below.

Recital 49:

***The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist**, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and **the security of the related services offered by**, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by **providers of security technologies and services, constitutes a legitimate interest of the data controller concerned**. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.*

The above Recital underpins the legitimacy of iProov retaining and processing data for the purposes of sustaining the security of its systems and processes in addition to the biometric information which is collected under the service. Since the uses iProov makes of this data are legitimate, the processing is lawful as it is a key part of the service provided by Iproov.

The requirements for fairness and transparency are satisfied by an adequate disclosure of the uses of the data, as part of a consent process, and by
appropriate measures to prevent discrimination, in compliance with the terms of Recital 71:

*In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, **the controller should use** appropriate mathematical or **statistical procedures** for the profiling, **implement technical and organisational measures appropriate** to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and **that***

***prevents**, inter alia, **discriminatory effects on natural persons on the basis of racial or ethnic origin**.*

This Recital sustains the legitimacy and necessity of processing and storing data for the purposes of preventing racial or ethnic discrimination, as part of the purposes for which consent is to be given by the Data Subject. We interpret “inter alia” to include also discriminatory effects on the basis of gender or age.

5.2 Purpose Limitation

When serving a Data Controller who retains control of the Data Subject identity, iProov is strict in using the data it collects under the instructions of the Data Controller solely for the purposes of:

- delivering its service of authentication
- detection, analysis and prevention of suspected fraud or patterns of fraud
- actions taken to maintain the security, accuracy and non-discriminatory reliability of its service of authentication whilst not impairing its reliability

These are essential and lawful uses for the data, and no other use is made of the Personal Data when processing on behalf of a Data Controller.

5.3 Data Minimisation

When serving a customer retaining control of the Data Subject identity, iProov meets the Data Minimisation principle by:

- Storing and processing data from fraudulent claims in a pseudonymised form for a default period of **one year**.
- Storing and processing data from genuine but unsuccessful claims for the time required to determine failure causes and correct them in order to improve the security, accuracy and non discriminatory reliability of the service. This retention period is by default up to **three months**.
- Storing and processing imagery from successful authentications only to the extent necessary to enable the Data Controller to establish and demonstrate that the system exhibits no bias on age, gender or ethnicity. **This period is by default one month** for any single sample, and three months in the case that bias is detected and must be removed.
- Declining to accept any information that might identify the natural person, and deleting immediately any such information that is received. All Personal Data is pseudonymised by design, as recommended by Recital 28 and Article 25.
- Storing and processing records of users for the duration of the purpose when this is a prolonged or indefinite period of time, such as for use in repeat authentication, in a form that cannot be recognised by a person and cannot reasonably be reverse engineered to produce human-readable imagery.

5.4 Accuracy

Data accuracy is essential for the delivery of Verifier, iProov's face verification service. To prevent inaccurate data polluting the records of a Data Subject, the analysis of suspected fraud attempts is essential. Only data with a high degree of confidence is allowed to increment the Data Subject's records.

iProov's ID Matcher service does not use the personal data of a legitimate user for the purpose of delivering any further service to the Data Subject or the Data Controller, so the Core Principle requirement of data accuracy is not relevant.

5.5 Storage Limitation

iProov stores data for no longer than is strictly necessary, in its judgment, for the purposes to which consent has been given by the Data Subject or as justified by a lawful basis for retaining the data . The Storage Limitation principle applies the same rules from data minimisation.

5.6 Security, Integrity & Confidentiality

iProov operates under an ISO 27001 certified Information Security Management System (ISMS) to protect the security, integrity and confidentiality of all personal data and processing in its entire organization. This is subject to audit every twelve months, and processes are regularly updated to reflect the evolution of the business.

iProov's service is hosted in a number of cloud platforms including Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP) which itself has a full range of certifications, both logical and physical, to underwrite the protection of the personal data stored and processed by iProov.

iProov complies with the requirements of Article 32 insofar as:

a) the pseudonymisation and encryption of personal data;

iProov pseudonymises all personal data and has no access itself to any information that might reverse this pseudonymisation. All Personal Data stored by iProov is encrypted.

Compliance with the remainder of Article 32 is provided by iProov's associated technical controls and infrastructure in accordance with its ISMS and ISO27001 certification.

5.7 Privacy by Design

Please see iProov Privacy by Design and Default policy for further information.

6. Consent

As indicated above, there is an obligation on Data Controllers to obtain explicit consent from users for the processing of any Special Category personal data for the purposes of authentication. The required consents for iProov's processing are for the following:

Processing any special category personal data for the purposes of:

- Authentication of the user
- Detection and investigation of suspected individual or systematic fraudulent behaviours
- Maintenance of the security, accuracy and usability of the system
- Fully automatic authentication decisions (recommended)

Such consents are required for the following reasons:

6.1 Special Category Status

As noted in Section 2, facial imagery used for authentication may constitute Special Category Personal Data. The processing of such data is forbidden except under the provisions of Article 9.2. The most generally applicable of these is 9.2(a) – explicit consent. Without such consent, a convincing case would have to be made for a legitimate basis for processing under another part of Article 9, such as 9.2(e) – data manifestly made public. Whilst this may in future be debated, iProov does not believe this is a sustainable basis for processing at this time, in part because it does not qualify as a basis for automated individual decision making.

6.2 Obtaining Consent

Data Controllers are responsible for obtaining and managing any consent from the Data Subjects according to the requirements of the GDPR. This requirement will apply to any attempt to use Special Category data by any technical means, local or cloud-based, and is not specific to iProov services.

The regulations on "consent" in the GDPR are as follows:

Recital 32:

*Consent should be given by a clear **affirmative act** establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data*

relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical
settings for information society services or ***another*** *statement or* ***conduct which clearly indicates in this context the data subject's acceptance*** *of the*
proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. ***Consent should cover all processing activities carried out for the same purpose*** *or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.*

Guidance on the meaning of "explicit consent" is being developed by the Article 29 Working Group (in future the European Data Protection Board).

The requirement to show, and permit the withdrawal of, consent is specified as follows:

Article 7:

1. *Where processing is based on consent, the controller shall be* ***able to demonstrate*** *that the data subject has consented to processing of his or her personal data.*
2. *If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*
3. *The data subject shall have the* ***right to withdraw his or her consent at any time****. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof.* ***It shall be as easy to withdraw as to give consent.***

7. iProov's Responsibilities

iProov is a Data Processor, acting as a processor of personal data for the Data Controller under a contract which is the client of iProov or of our partners.

Therefore, under Article 29:

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Under Article 28, iProov's contracts with Data Controllers must comply with the following mandatory requirements:

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and 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 controller. That contract or other legal act shall stipulate, in particular, that the processor:

A. *processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*
B. *ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;*
C. *takes all measures required pursuant to Article 32 (Security of Processing);*
D. *respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;*
E. *taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for*
F. *exercising the data subject's rights laid down in Chapter III (Rights of the Data Subject);*
G. *assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Security, Data Breach, Impact Assessment, Prior Consultation) taking into account the nature of processing and the information available to the processor;*
H. *at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;*
I. *makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and*
J. *contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.*

iProov notes that:

- under Article 82(2) it is liable for the damage caused by its processing only *"where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."*.
- Article 82(4) creates several liability for non-monetary damage caused by processing and hence a potential liability on iProov for the actions of the Data Controller or other Data Processor.
- Article 82(5) creates an explicit right in law for the processor to be reimbursed by the Controller or other Processor for damages corresponding to their responsibility arising under this liability, and this will be recognised by indemnification provisions in iProov's contracts with its clients.

7.1 Mitigation of Administrative Action Risks

iProov recognises that a Data Controller might hypothetically be exposed to administrative action under Article 83 as a result of an action or inaction of iProov. However the provisions of Article 83(2) on the factors affecting such a fine are such as to minimise the liability of iProov, since

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

iProov considers it likely that the nature, gravity and hence damage caused to users by the compromise of the pseudonymised, unidentifiable face images it holds will not be considered material by the supervisory bodies. The iProov technology is designed to prevent the successful reuse of such imagery in an iProov authentication process, and iProov does not hold any data that might assist in the identification of the person who was the original subject of the imagery.

(b) the intentional or negligent character of the infringement;

iProov will never be complicit and intends never to be incompetent in its stewardship of Personal Data.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

iProov's ISO 27001 ISMS covers the company's response to a breach. Damage suffered will be mitigated by the pseudonymisation and encryption of all data held by iProov.

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

iProov will cooperate fully with any supervisory authority.

(g) the categories of personal data affected by the infringement;

All Personal Data held by iProov is pseudonymised and encrypted.

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

iProov will always proactively notify promptly of a breach or infringement to the Data Controller in accordance with the requirements of Article 33(2).

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;

At this time there are no approved codes of conduct. iProov is monitoring their development and intends to adhere to relevant codes when they become available.

7.2 Breach Notification

iProov notes that Article 34.3(a) exempts Data Controllers from the obligation to notify a Data Subject if the personal data affected by the breach has been encrypted. All iProov data is encrypted.

Whilst Article 33 exempts notification of a breach to a supervisory authority by a Data Controller if it *"is unlikely to result in a risk to the rights and freedoms of natural persons"*, iProov will always notify the Data Controller of personal data breaches, irrespective of the wording of this exemption.

7.3 Data Subject Rights

If the right of access under Article 15 or the right to be forgotten under Article 17 is legitimately invoked by the Data Subject, then iProov will reasonably assist the Data Controller if it is in a position to comply with the Data Controller's request, provided the Data Controller supplies the pseudonym of the Data Subject necessary for iProov to identify their records if it is unable to comply with the Article 15 or 17 request itself.

8. Data Protection Officer

Since iProov's core activities include the large-scale processing of data that may be considered Special Category personal data, in compliance with Article 37 iProov has appointed a Data Protection Officer who can be contacted at dpo@iproov.com.

Document Owner & Approval

The Chief Technology Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS and iProov remains compliant.

The current version of this document is available to all members of staff electronically.

This document is approved by the CEO on the issue date shown and is issued on a version controlled basis.

Version Number	Nature of Issue	Author	Approver	Date of issue
1.0	Initial release	Andrew Bud	Andrew Bud (AB)	04/2016
1.1	Review	Dominic Forrest (DF)	AB	03/2017
1.2	Review	DF	AB	11/2017
1.3	Review	Martin Dooley (MD)	DF	04/2018
2.0	Rewrite with new DPA law	DF	AB	06/2018
2.1	Review	DF	AB	02/2019
2.2	Review and small alterations	MD	DF	08/2019
2.3	Review	MD	DF	05/2020
2.4	Review	Nilma Bonelli (NB)	DF	02/2021
2.5	Review and small corrections	NB	DF	11/2021
2.6	Review	NB	DF	10/02/2022
2.7	Review, minor changes	NB	DF	08/02/2023