iCHECK CANDIDATE PRIVACY NOTICE

last updated: 19/10/2026

Table of Contents

1. Introduction....2
2. Processing and deletion of personal data....3
    2.1. Personal data we collect....3
        2.1.1. Identification document data....3
        2.1.2. Biometric data....3
        2.1.3. Address data....4
        2.1.4. Contact, session and technical data....4
    2.2. Personal data we report to our clients....4
    2.3. Deletion of personal data....5
    2.4. Legal basis for the processing....6
    2.5. Screening Checks....6
3. Fraud prevention agencies....8
4. Transfer of personal data....8
5. Automated decisions....9
6. Security measures....10
7. Your rights....10
8. Children's Privacy....12
9. General provisions....12

 ©2026 iCOVER Group. All rights reserved.

1. Introduction

The iCOVER Group (the "iCOVER Group") is a French-headquartered group specialised in international verification services, backed by a network of offices worldwide. The iCheck platform ("iCheck") is operated by I-Cover (Screening) Limited, a company registered in England and Wales under company number 06643359, with its registered office at 30 Old Bailey, London EC4M 7AU ("iCOVER", "we" or "us").

Through iCheck we provide our clients (the organisations that invite you to complete a check, such as an employer, recruiter, letting agent or DBS umbrella body) with a candidate verification journey. Depending on what our client has ordered, your journey may include:

- identity verification ("IVS"): a check of your identity document, a biometric liveness and face match check, and an address check. IVS supports digital Right to Work, Right to Rent and Disclosure and Barring Service (DBS Basic and Standard) identity checks; and
- additional background screening checks that our client adds to your journey, such as criminal record, education, employment or media checks ("Screening Checks"). These are carried out through our background screening system (see section 2.5).

In this Notice, "you" means the person invited to complete a check. IVS is built as per the rules set out in the UK Digital Identity and Attributes Trust Framework ("UKDIATF") under the Data (Use and Access) Act 2025 and is maintained by the Office for Digital Identities and Attributes, and allows one-time verification of an individual's identity. iCheck is certified against this framework as an identity service provider for Right to Work, Right to Rent and DBS, profiles M1D, M2B, H3A .

This privacy notice (the "Notice") is provided in compliance with the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018, the General Data Protection Regulation ("GDPR") and any data protection law applicable in your jurisdiction (the "Data Privacy Laws"). We are firmly committed to respecting your right to privacy and taking seriously our responsibilities concerning the processing of your personal data. This Notice provides you with information regarding the processing of your personal data when you are invited to complete a check through iCheck and sets out important information about your rights. It does not replace the privacy notice of the organisation that invited you, which explains how that organisation uses your information.

This Notice applies to personal data we process in the course of providing iCheck, regardless of where you are located. If you reside outside the UK or EU, you may have different privacy rights and protections under the laws of your country.

If you have any questions about this Notice or want to exercise your rights set out in this Notice, please contact us by sending an email to privacy@icover-services.com.

 ©2026 iCOVER Group. All rights reserved.

2. Processing and deletion of personal data

While providing iCheck, our client engages us to help it verify the identity of a living person (you) during a one-time transaction to confirm you are a real person and not someone trying to impersonate you, and, where ordered, to carry out Screening Checks.

Our client is the controller of your personal data and we act as its processor. This means that Our client decides who will undergo a check; for what purpose; which checks are carried out; the legal basis for processing your personal data; and how your information is collected, used, shared and retained by it. We process your personal data only on our client's documented instructions, under a written data processing agreement, and not for our own purposes, except in the limited cases described in section 2.4. Our client should have given you its own privacy notice explaining this. If you have not received it, please ask the organisation that invited you.

2.1. Personal data we collect

Personal data collected for the purpose of the IVS include:

2.1.1. Identification document data

What? Full name, date of birth, place of birth, nationality, address, document type and number, document issuing country, issue and expiry dates, photo, MRZ code, the other data read from the document, and images of the front and back of your document.

How? You capture images of your identity document with your device camera, and the data is extracted from it and the document is checked for signs that it is genuine and valid (for example its layout, security features and expiry date) so that your identity can be verified.

Why? This is the base against which we will conduct the liveness face match check, by comparing the document portrait and the video selfie.

2.1.2. Biometric data

What? Biometric data derived from images of your face: a short video selfie, and facial templates created from it and from the photo on your identity document.

How? A short video selfie is recorded on your device so that a liveness verification (confirming that a real, live person is present) and a check that the video has not been manipulated or injected is performed.

Why? An image of your face ("face template") is extracted from the video and compared with the photo extracted from your identity document. These checks are carried out automatically (see section 5).

If you do not want to use the biometric check. You do not have to give consent to biometric processing. If you prefer not to, select 'Cancel' on the consent screen. A message will tell you that your verification

 ©2026 iCOVER Group. All rights reserved.

in iCheck will be cancelled. You can then ask for the alternative route by contacting either the organisation who has asked you to do the verification or us here.

2.1.3. Address data

What? Current address and the date from which you have lived there.

How? We collect your current address from the details you enter in the journey and from information in a proof of address document you upload (for example a utility bill, bank or credit card statement, or mortgage statement). We compare it to the address held by Experian, a credit reference agency, using its CrossCore service. . We may also use an address validation service to check that the address you enter exists, and a document fraud detection service to check that the proof of address you upload has not been altered.

Why? To confirm your current address.

2.1.4. Contact, session and technical data

What? Your name and email address, the PIN you create to resume your journey (stored only as a hash, so we cannot retrieve it or send it to you again) and the approximate location derived from it, and records of your journey (for example when you were invited, which steps you completed, and the declarations you confirmed and when).

How? Our client provides your name and email address when it orders the check. The other information is collected automatically as you use iCheck.

Why? To send you your invitation and journey emails, to let you resume your journey securely, to keep iCheck secure, and to keep an audit record of the check, which our client and our certification require.

Upon completion of the identity verification service, a report is provided to our clients to assist them to conduct digital identity verification checks for different purposes, these could include but are not limited to “Disclosure and Barring Service”, “Right to Work” and “Right to Rent” checks.

2.2. Personal data we report to our clients

Personal data included in the report:

- General information: first name, middle name, last name, current address, the date from which you have lived there, date and place of birth;
- Identity document information: type, issuing country, date of issue and expiry date, [document number and MRZ code];
- Verification information: the overall verdict, the result of each check (document authenticity, liveness, face match, image and video validation, and address history), the identity confidence profile achieved (for example M1D, M2B or H3A), and the reason for failure (if any); and
- where our client has asked for them, copies of the images and files you provided, such as your document images and proof of address.

 ©2026 iCOVER Group. All rights reserved.

Our client's authorised users can see the result in the client dashboard.

2.3. Deletion of personal data

Once the check is completed and the report is issued, we delete your personal data in accordance with the data retention period defined by our client (for Right to Work, Right to Rent and DBS checks, these periods are pre-defined to meet the requirements of our certification); and in any event, we do not retain your data for more than the retention periods indicated below:

	Verification successful	**Verification not successful**	**Verification not successful and including a fraud suspicion**
Identification Document data	3 days from the closing of IVS	30 days from the closing of IVS	Only for the time strictly necessary to investigate the suspicion and meet legal or regulatory obligations
Biometric data	3 days from the closing of IVS	30 days from the closing of IVS	Only for the time strictly necessary to investigate the suspicion and meet legal or regulatory obligations
Address data	3 days from the closing of IVS	30 days from the closing of IVS	Only for the time strictly necessary to investigate the suspicion and meet legal or regulatory obligations
Supporting documents (such as proof of address)	3 days from the closing of an Identity Verification Service	30 days from the closing of an Identity Verification Service	Retained only for the time strictly necessary to investigate the suspicion and fulfil legal or regulatory obligations

©2026 iCOVER Group. All rights reserved.

In any event, we delete your personal data held in iCheck no later than thirty (30) days after the check is closed, which is the maximum amount of time that we can have access to your personal data, unless there is a legal or regulatory reason that prevents us from deleting it, for instance, if we suspect a fraudulent document that we may need to share with fraud prevention agencies or disclose upon request to law enforcement authorities. Personal data that our client has received from us is kept by our client in line with its own retention policy. If you start but do not finish your journey, your invitation stays open for 30 days or the period set by our client. For identity verification, an incomplete journey may be closed after 7 days, after which your data is deleted in line with the table above. For ID and Biometric checks we retain the results without any associated personal information for three years.

2.4. Legal basis for the processing

We process your personal data as a data processor on behalf of our clients, under a service agreement and data processing agreement with each client. As a processor, we do not choose the legal basis for this processing. Our clients determine the legal basis for the processing of your personal data, and explain it in the privacy notice that they have communicated to you.

Where our client relies on your consent, iCOVER collects that consent on behalf of our client. In particular, our client relies on your explicit consent for the processing of biometric data, which we ask for on a dedicated screen before any facial scan is captured. You give this consent to our client, and we record it on our client's behalf. You may decide not to give your consent; in this case, you will be offered the alternative route described in section 2.1.2.

Limited cases where we act as controller. In a small number of cases we use your personal data for our own purposes, and for those purposes only we are a controller:

- to report confirmed or suspected fraud to fraud prevention agencies where the reporting criteria are met (see section 3);
- to respond to lawful requests from law enforcement or regulatory authorities, and to meet our own legal and regulatory obligations;
- to keep the records we need to evidence our certification under the trust framework, and to establish, exercise or defend legal claims; and
- to keep iCheck secure, including detecting and preventing misuse of the platform.

For these purposes we rely on our legitimate interests in preventing fraud and operating a secure, certified service and, where applicable, on compliance with a legal obligation. Where special category data such as biometric data is involved, we rely on the substantial public interest in preventing or detecting unlawful acts and preventing fraud or defence of legal claims

2.5. Screening Checks

If our client has added Screening Checks to your journey, we carry them out on our client's behalf, on the same processor basis described above, using our internal background screening system. You will not

 ©2026 iCOVER Group. All rights reserved.

use this system directly. The information you provide in iCheck, such as your identity details and the result of your identity check, is used to complete the checks our client has ordered.

We offer many types of Screening Check and add new ones over time. Some of them are listed below in a broad list. Our client decides which checks apply to you and should explain this in its own privacy notice. The checks ordered for you are also shown in your journey.

Category of check	**Personal data used**	**Who we may contact or search**
Criminal record checks	Identity details, address history, and criminal record information returned by the check	The Disclosure and Barring Service or equivalent official bodies in other countries
Employment history and references	Employment dates, job titles, reason for leaving, referee details	Former employers and referees you name
Education and professional qualifications	Qualifications, institutions, dates, membership numbers	Universities, schools, examination and professional bodies
Financial and directorship checks	Identity details, address history, court judgments, insolvency and directorship records	Credit reference agencies and public registers
Sanctions and watchlist checks	Name, date of birth, nationality	Official sanctions lists and screening databases
Media checks	Name and other identifiers needed to match results to you	Publicly available news and media sources

Some checks can reveal information about criminal offences or other sensitive matters. We only carry out these checks where our client has confirmed it has a lawful basis to request them, and we use the results only to report to our client.

The results of Screening Checks are returned to our client and kept for the retention period our client sets.

©2026 iCOVER Group. All rights reserved.

3. Fraud prevention agencies

Routine fraud check. As a standard part of every identity check, we search your core identity details (your name, date of birth, address and IP address) against the Cifas National Fraud Database. The personal information we have collected from you will be shared with fraud prevention agencies who will use it to prevent fraud and money laundering and to verify your identity.

Fraud reporting. If our fraud team confirms, after investigation, that the criteria for reporting to Cifas are met, we will record this with Cifas. If fraud is detected, you could be refused certain services, finance, or employment by Cifas members.

For UK: further details of how your information will be used by us and these fraud prevention agencies, together with your data protection rights, see the Fair Processing Notices for Cifas (https://www.cifas.org.uk/fpn). You can contact Cifas directly if you want to dispute a Cifas record.

Elsewhere: If you are located outside the UK, we may share your information with local equivalents of fraud prevention agencies, credit bureaus, or other governmental authorities only if required by law. We will only do so in compliance with applicable data protection regulations. For more information specific to your jurisdiction, please contact us.

4. Transfer of personal data

Where your personal data is transferred outside the UK or the European Economic Area, we make sure it is protected by an appropriate safeguard. These include the UK International Data Transfer Agreement (IDTA), the UK Addendum to the European Commission Standard Contractual Clauses (SCCs), the SCCs themselves for transfers from the EEA, and transfers to countries recognised as providing adequate protection. We also assess the risks of each transfer. You can ask us for more information about these safeguards.

We transfer or may transfer your personal data to:

- **Our client.** We perform the check on its behalf and provide it with a report;
- **Law enforcement authorities.** Upon a law enforcement or regulator's request, we may be obliged to disclose personal data. We carefully validate these requests, including reviewing the legality of any order and challenging the order if there are grounds under the law to do so, before any personal data is disclosed ;
- **Fraud prevention agencies**. For the UK, we search the Cifas National Fraud Database as part of every check and, in case we have a fraud suspicion, we will investigate and, if the investigation meets the criteria for reporting, report it to Cifas. For more information about Cifas, you can click HERE (https://www.cifas.org.uk/contact-us) or refer to the "Fraud Prevention Agencies" section;
- **Third-party service providers** (our sub-processors) that help us deliver iCheck, listed in the table below. They act only on our instructions and are bound by written contracts that protect your data.

 ©2026 iCOVER Group. All rights reserved.

Provider	What it does	Personal data involved
Unissey	Liveness detection and face matching	Video selfie, document photo, facial templates
Experian Ltd	Address and identity verification (CrossCore)	Name, date of birth, address

In addition, the following iCOVER Group companies support us in delivering iCheck, for example by carrying out manual reviews, and may access your personal data for that purpose: (BULGARIA) ICOVER SERVICES EOOD; (FRANCE) SQUARE FACTS SAS; (INDIA) ICOVER INDIA INFORMATION AND SERVICES PRIVATE LIMITED.

Information for California residents. We do not sell your personal information as the terms "sell" and "personal information" are defined by the California Consumer Privacy Act (the "CCPA"). Any questions or requests regarding the processing of your personal information in respect of your rights under the CCPA should be directed to privacy@icover-services.com.

5. Automated decisions

- the liveness check and the face match between your video selfie and your document photo are fully automated;
- your document is checked automatically. If no valid identity document can be detected in your images, or the document does not meet the requirements of the check, you will be asked to try again. If the second attempt also fails, your check will be closed automatically [and reported to our client as unsuccessful]; and
- if the automated checks raise an alert on your identity document, a trained member of our fraud team reviews it before a result is issued.

Our client receives the result and decides what it means for you, for example whether to proceed with your application. Because the automated biometric checks use your biometric data, they are carried out only with your explicit consent.

Our use of AI tools. Separately from the automated checks described above, we use artificial intelligence ("AI") tools to support certain steps in delivering iCheck and Screening Checks. These tools are provided by third party AI providers under Zero data retention agreements and are built into our own workflow tools. Depending on the checks ordered for you, they may be used to extract text from the documents you provide, to classify those documents and check that they are complete and of sufficient quality, to help detect signs that a document has been altered, and, for Screening Checks, to filter media and public record search results (such as court records) to identify those that may relate to you. This means the AI tools may process your identity details (such as your name, date of birth, address and nationality), the content of your documents and publicly available information about you. These AI tools do not make decisions about you. Their output supports our trained analysts: any check that the AI tools cannot complete with sufficient confidence is passed to an analyst, and any adverse result is

 ©2026 iCOVER Group. All rights reserved.

reviewed by an analyst before it is reported to our client. The AI Providers process your personal data only on our instructions and under zero-data-retention arrangements, which means they do not keep your personal data or use it to train their AI models. You can exercise the rights described below and in section 7 in relation to any result supported by AI tools.

You have the right to be told about an automated result, to make representations, to ask for a person to review it, and to contest it. In this case, please contact us here. and your verification will be reviewed by a member of our team who has the authority to change the result. You can also contact the organisation that invited you, as it is responsible for the decisions it makes using the result.

6. Security measures

We use accepted standards of physical and technical measures and require our hosting partners to use the same standard of care to protect personal information. Despite our best effort to protect personal information, the transmission of information via the internet is not completely secure. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access. More information about our security measures can be found in our Main Privacy Policy (see section 9).

We also maintain procedures to identify, respond to, and resolve any suspected personal data breaches. We will notify our client without undue delay if we become aware of a personal data breach affecting your data, and we will help our client to notify the relevant regulator and you where this is required by law. Where we act as controller (see section 2.4), we will notify the regulator and you ourselves where required. If you believe your information may have been compromised or if you notice any suspicious activity, please contact us immediately at privacy@icover-services.com.

7. Your rights

Because our client is the controller of your personal data, it is responsible for responding to requests to exercise your rights, and you can contact the organisation that invited you directly. If you contact us instead, we will pass your request to our client promptly [within 2 working days] and help it to respond. Where we act as controller (see section 2.4), we will respond to you directly.

You have the following rights in relation to the personal information we hold about you:

Your right of access or Subject Access Request: If you ask us, we'll confirm whether we're processing your personal information and, if necessary, provide you with a copy of that personal information (along with certain other details). If you require additional copies, we may need to charge a reasonable fee. We do not have to share information about fraud indicators where this would prejudice the prevention or detection of fraud. For information held by a fraud prevention agency, please contact that agency directly.

Your right to rectification: If the personal information we hold about you is inaccurate or incomplete, you are entitled to request to have it rectified. If you are entitled to rectification and if we've shared your personal information with others, we'll let them know about the rectification where possible. If you

 ©2026 iCOVER Group. All rights reserved.

ask us, where possible and lawful to do so, we'll also tell you who we've shared your personal information with so that you can contact them directly.

Your right to erasure: You can ask us to delete or remove your personal information in some circumstances such as where we no longer need it or if you withdraw your consent (where applicable). If you are entitled to erasure and if we've shared your personal information with others, we'll let them know about the erasure where possible. If you ask us, where it is possible and lawful for us to do so, we'll also tell you who we've shared your personal information with so that you can contact them directly.

Your right to restrict processing: You can ask us to 'block' or suppress the processing of your personal information in certain circumstances, such as where you contest the accuracy of that personal information or you object to us. If you are entitled to restriction and if we've shared your personal information with others, we'll let them know about the restriction where it is possible for us to do so. If you ask us, where it is possible and lawful for us to do so, we'll also tell you who we've shared your personal information with so that you can contact them directly.

Your right to data portability: You have the right, in certain circumstances, to obtain personal information you've provided us with (in a structured, commonly used and machine-readable format) and to reuse it elsewhere or to ask us to transfer this to a third party of your choice.

Your right to object: You can ask us to stop processing your personal information, and we will do so, if we are: (i) relying on our own or someone else's legitimate interests to process your personal information, except if we can demonstrate compelling legal grounds for the processing; or (ii) processing your personal information for direct marketing purposes.

Your right to withdraw consent: If our client relies on your explicit consent as its legal basis for processing your personal information, you have the right to withdraw that consent at any time. In this case, we will stop the biometric processing and you will be offered the alternative route described in section 2.1.2. Withdrawing consent does not affect processing already carried out.

Your right to lodge a complaint with the supervisory authority: If you have a concern about any aspect of our privacy practices, including the way we've handled your personal information, you can report it to the relevant supervisory authority

Please note that some of these rights may be limited where we have an overriding interest or legal obligation to continue to process the data.

For non-UK/EU residents, your rights may vary. Please refer to your local data protection authority for specific rights and obligations that may apply to you.

To exercise your data privacy rights, please email privacy@icover-services.com. We will acknowledge your request within 96 hours. Where we pass your request to our client, our client will respond within the time required by law (usually one month). Where we respond ourselves, we will do so within one month.

©2026 iCOVER Group. All rights reserved.

8. Children's Privacy

Our clients decide who is invited to complete a check. Some checks can involve people under 18. If you are under 18, your data is processed in the same way and with the same protections described in this Notice, and our client is responsible for making sure that the check is appropriate for you. A parent, guardian or other trusted adult can contact us or the organisation that invited you on your behalf if you have questions.

9. General provisions

Amendments. Any changes made to this Notice from time to time will be published on iCheck and at iCheck Privacy Policy. Any material or other change to the data processing operations described in this Notice that is relevant to or impacts on you or your personal data will be notified to you. In this way, you will have an opportunity to consider the nature and impact of the change and exercise your rights under the UK GDPR or GDPR in relation to that change (e.g., to withdraw consent or to object to the processing) as you see fit.

Main Privacy Policy. For more detailed information on our global data protection practices, please see our Main Privacy Policy at Privacy Policy - iCover. Please note that the Main Privacy Policy excludes biometric data, which is covered by this dedicated Notice.

Contact. If you have any comments or questions about this Notice or our processing of your information, please contact our Data Protection Office at privacy@icover-services.com, or write to: Data Protection Office, iCOVER Group, 1 rue de la Bourse, 75002 Paris, France

Complaint. For further information on the protection of personal data or the issuing of a complaint, you can visit:

- the website of the Information Commissioner's Office ("ICO"), https://ico.org.uk/ where we are registered under number Z1637061; or
- the website of the Commission Nationale de l'Informatique et des Libertés ("CNIL"), www.cnil.fr, if your data is processed by one of our EU group companies or you are located in the EU

We are available for you and we would appreciate the chance to deal with your concerns as a first step before you approach the Data Protection Authority. Please do not hesitate to contact us at privacy@icover-services.com.

©2026 iCOVER Group. All rights reserved.