

Quicker DBS

Privacy Policy

Last updated: 22/09/2026

Who provides this service

Legal entity: Aaron's Department

Company number: 05004030

Registered office: 43 Church Lane, Pudsey, LS28 7RR

ICO registration number: ZB176923

Website: www.aaronsdepartment.com

Data Protection Contact: data-protection@aaronsdepartment.com

This Privacy Policy explains how the legal entity identified above ("we", "us" or "our") collects, uses, stores, shares and protects personal information.

It applies to our websites, online accounts, portals, applications and services, including screening, verification, employment, identity, compliance, driver and vehicle, tachograph, training, workforce management, onboarding, checklist, document-management and related business services and digital tools.

We provide a wide and developing range of services. Not every part of this Privacy Policy will therefore apply to every service, and not every service collects every category of information described below.

Where a particular service requires additional information about how personal information is processed, we may provide a supplementary or just-in-time privacy notice when that service is used. Any such notice should be read together with this Privacy Policy.

1. Data protection law

We process personal information in accordance with applicable data protection and privacy legislation, including the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), the Privacy and Electronic Communications Regulations 2003 ("PECR"), and legislation which amends or supplements those laws, including the Data (Use and Access) Act 2025.

This Privacy Policy is intended to provide the privacy information required by data protection law.

It is not a contract and acceptance of this Privacy Policy is not itself the legal basis on which we process personal information.

When you create an account or begin using a service, you may be asked to confirm that you have read and understood this Privacy Policy and any additional privacy information relevant to the service.

Separate contractual terms may also apply.

2. When we are a controller and when we are a processor

Our role depends on the service being provided and who has commissioned it.

2.1 Services commissioned by an organisation

Where an employer, prospective employer, customer or other organisation ("Client") asks us to provide a service concerning an applicant, worker, employee, driver or other individual, the Client will usually determine why the information is being processed and the service it requires.

For personal information that we process solely on the Client's instructions, the Client is normally the **data controller** and we act as its **data processor**.

This may include information processed in connection with:

- employment and background screening;
- DBS and other permitted checks;
- identity and Right to Work verification;
- references;
- driver and licence checking;
- tachograph and working-time analysis;
- vehicle and location services;
- onboarding;
- employee and workforce tools;
- checklists and inspections;
- document-management and document-storage services;
- training and competency records; and
- other screening, compliance and business services.

Where we act as processor, the Client is responsible for determining its lawful basis for the processing, deciding what information it requires and determining appropriate retention periods, subject to applicable law and our contractual arrangements.

2.2 Our own processing

We may also act as a **controller in our own right** for activities such as:

- creating and administering accounts;
- information and system security;
- access control;
- audit records;

- fraud prevention;
- regulatory and legal compliance;
- billing;
- customer and technical support;
- service administration;
- dealing with complaints and legal claims; and
- our own business communications and marketing.

2.3 Services purchased directly by an individual

Where an individual purchases a service directly from us, we will normally act as the controller for the information necessary to provide and administer that service.

It is therefore possible for us to act as a processor for one activity and a controller for another.

3. Who this Privacy Policy covers

This Privacy Policy may apply to:

- visitors to our websites;
- customers and prospective customers;
- Client administrators and authorised users;
- applicants and prospective workers;
- employees and workers;
- drivers;
- self-employed individuals;
- referees and reference providers;
- directors, business owners and officers;
- trainees and course participants;
- suppliers and professional contacts;
- individuals whose information is supplied to us by a Client;
- people contacting our support, sales or administration teams; and
- business contacts to whom we market our services.

4. Personal information we may process

The information we process depends upon the service involved.

We intend only to collect information which is relevant and reasonably necessary for the relevant purpose.

4.1 Identity, contact and biographical information

This may include:

- name and previous names;
- title;

- date of birth;
- place of birth;
- gender where relevant to a particular check or service;
- residential address and previous address history;
- email address;
- telephone number;
- nationality;
- photograph;
- signature;
- business details;
- job title;
- employment status; and
- identifiers allocated to an account, service or application.

4.2 Account, device and security information

This may include:

- usernames and account identifiers;
- authentication information;
- account permissions;
- login history;
- Internet Protocol (IP) addresses;
- browser information;
- device information;
- operating-system information;
- security events;
- access logs;
- audit history;
- timestamps; and
- records of changes made to information.

We may record which applicant, authorised Client user, evidence checker, countersignatory or other person created, amended, reviewed or returned information.

4.3 Identity documents and verification information

Depending upon the service, we may process information contained in or derived from documents including:

- passports;
- driving licences;
- birth certificates;
- immigration documents;
- eVisa evidence;
- proof-of-address documents;
- financial documents supplied as evidence;
- photographs; and

- other documents provided as evidence of identity.

We may also process:

- identity-verification results;
- document-authenticity results;
- electronic identity-check results; and
- information returned by external identity-verification providers.

Actual images of identity documents may be retained where required for a particular service.

4.4 Right to Work and immigration information

This may include:

- Home Office share codes;
- immigration status;
- permission to work;
- restrictions upon work;
- Home Office profile information;
- photographs;
- information returned by the Home Office service; and
- evidence demonstrating that a Right to Work check has been completed.

4.5 Employment, professional and reference information

This may include:

- current and previous employment;
- periods of employment;
- job titles and responsibilities;
- reasons for leaving;
- employment gaps;
- references;
- referee details;
- free-text reference responses;
- qualifications;
- education;
- training;
- professional memberships and registrations;
- competency records;
- certification records;
- directorships; and
- other information relevant to the particular screening, employment or onboarding service.

Reference providers may provide information in free-text form. Depending on what a referee chooses to disclose, this may occasionally contain sensitive information.

4.6 Background, screening and compliance information

Depending upon the service, we may process information obtained through:

- credit or financial checks;
- directorship searches;
- professional or regulatory registers;
- sanctions screening;
- politically exposed person screening;
- adverse-media searches;
- fraud-prevention checks;
- driving-licence checks;
- qualification checks;
- professional-registration checks;
- public records;
- publicly available internet sources; and
- social or professional networking sources where use of such information is lawful and relevant to the service.

4.7 DBS application information

We process information necessary to submit, administer and track eligible DBS checks, including as applicable:

- Basic DBS checks;
- Standard DBS checks;
- Enhanced DBS checks;
- Enhanced DBS checks with barred-list checks;
- DBS Update Service checks; and
- Adult First checks.

This may include:

- application information;
- identity and biographical information;
- information required to verify identity;
- application identifiers;
- DBS reference numbers;
- check type;
- application status;
- certificate number and date where provided to us;
- dates associated with the application; and
- the electronic DBS result indicator.

What DBS information we receive

We do not receive the contents of the applicant's DBS certificate from DBS.

We do not receive details of convictions or cautions shown upon the certificate.

For applications submitted electronically, DBS may provide us with an electronic result indicating:

"Certificate contains no information"

or

"Certificate contains information".

Where the certificate contains information, the electronic result does not tell us what that information is.

The DBS certificate is sent directly by DBS to the applicant at the correspondence address recorded on their application. This will normally be the applicant's home address but, where permitted, may be an appropriate nominated or "care of" address.

It is the applicant's decision whether to provide their DBS certificate to an employer or other organisation.

Our **document-management service is separate from our DBS system**. Documents stored or uploaded through that separate service do not form part of the DBS application environment merely because the same individual also uses a DBS service.

4.8 Driver, vehicle and tachograph information

Depending upon the service, this may include:

- driving-licence information;
- DVLA information;
- driver identifiers;
- vehicle registration and vehicle information;
- driver-card information;
- tachograph records;
- driving time;
- working time;
- rest periods;
- breaks;
- periods of availability;
- infringements or potential infringements;
- compliance information;
- journey information;
- precise or approximate location information;
- GPS information; and
- timestamps.

Our systems may analyse this information and produce reports, calculations or matters for review.

4.9 Inspection, checklist and evidence information

Some services allow Clients or their users to complete configurable checklists, inspections, onboarding processes or other workflows.

These may contain:

- responses to questions;
- observations;
- photographs;
- videos;
- documents;
- timestamps;
- precise or approximate location;
- signatures;
- acknowledgements;
- notes; and
- other evidence requested by the Client or provided by the user.

4.10 Workforce and employee information

Where a Client uses our workforce, employee-management, onboarding, rota, planning, checklist or related tools, the service may contain information such as:

- working hours;
- rotas;
- availability;
- absence records;
- sickness information;
- holiday records;
- performance information;
- training records;
- employment records;
- disciplinary information;
- expenses;
- timesheets;
- HR notes;
- uploaded documents; and
- information configured by the Client.

We normally process this information on behalf of the Client.

4.11 Document-management information

Document management is a **separate service from our DBS system**.

Where a Client uses a document-management, onboarding or related storage service, the Client may ask an individual to upload or retain documents for its own employment, compliance, HR, operational or record-keeping purposes.

These documents may include any information the Client lawfully decides it needs, such as:

- identity documents;
- employment documents;
- training certificates;
- qualifications;
- licences;
- policies and acknowledgements;
- HR documents;
- onboarding records; and
- other records relevant to the Client's relationship with the individual.

Where we provide this service on the Client's behalf, we normally act as processor and the Client determines why the documents are required, who may access them and how long they should be retained.

Documents retained in this service are not treated as DBS application documents unless they are separately and lawfully used for a DBS-related purpose within the DBS process.

4.12 Training information

This may include:

- training courses booked or undertaken;
- attendance;
- progress;
- assessment results;
- scores;
- completion information;
- certificates; and
- competency records.

4.13 Communications and support information

We may process:

- emails;
- telephone calls;
- recorded calls;
- live-chat conversations;
- support requests;
- support tickets;
- complaints;
- correspondence; and
- notes concerning enquiries or support.

4.14 Payment and transaction information

Where payment is required, payment providers may process payment-card or bank information.

We may receive:

- payment status;
- transaction references;
- amounts;
- refund information; and
- other information required to administer the transaction.

Full card or banking credentials may be processed directly by the payment provider and may not be available to us.

4.15 Website and marketing information

This may include:

- pages visited;
- referring pages;
- interactions with our websites;
- browser and device information;
- advertising and analytics identifiers;
- cookie information;
- marketing preferences;
- campaign information; and
- business contact information obtained from public or commercial sources.

Further information is provided in our separate Cookie Policy.

5. Special category information and identity verification

Some categories of personal information receive additional protection under data protection law.

These include information concerning:

- health;
- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership;
- genetic information;
- biometric information used for the purpose of uniquely identifying somebody;
- sex life; and
- sexual orientation.

Some Client-configured workforce, onboarding, employee, document-management or checklist services may contain this information where the Client has lawfully decided that it is necessary.

Where we process this information solely on behalf of a Client, the Client is responsible for determining an appropriate lawful basis and Article 9 condition.

Users should not provide special category information through free-text fields or upload it to a service unless it has been requested for a legitimate purpose or is genuinely necessary for the service concerned.

5.1 Digital identity verification

We use external identity-verification providers for some services.

Depending upon the identity-verification method used, a provider may use technologies such as:

- facial comparison;
- selfie-to-document comparison;
- liveness verification;
- document authenticity checking; and
- other digital identity-verification techniques.

Where biometric information is technically processed for the purpose of uniquely identifying an individual, it is special category personal information under UK data protection law.

The external provider may process photographs or biometric information to carry out the verification.

We normally receive the verification result and associated personal information, which may include the applicant's photograph.

We do not ordinarily require the biometric template generated by the identity provider.

Where electronic identity verification cannot be successfully completed, an applicant may be able to use an appropriate manual or documentary verification route.

6. DBS result information

We do **not** ask applicants to provide details of convictions or cautions as part of our DBS application processing.

We do **not** receive the contents of the DBS certificate from DBS and cannot view the convictions, cautions or other information which may be shown upon it.

We receive only the limited electronic DBS result indicator described in section 4.7.

Where we act as processor on behalf of a Client, the Client is responsible for determining the lawful basis and other legal conditions applying to its use of that result, and we process it in accordance with the Client's documented instructions and our own legal obligations.

Receiving an electronic indication that a certificate contains information does **not** enable us to see what that information is.

We do not determine whether a person should be recruited, employed, retained or otherwise accepted merely because a certificate contains information.

That decision remains with the applicant and the organisation responsible for making the relevant employment, recruitment or other decision.

7. Where we obtain personal information

We may receive personal information:

- directly from you;
- from a Client;
- from your employer or prospective employer;
- from another authorised user acting for a Client;
- from referees;
- from current or previous employers;
- from the Disclosure and Barring Service;
- from the Home Office;
- from the DVLA;
- from identity-verification providers;
- from qualification providers;
- from professional and regulatory bodies;
- from credit, fraud, sanctions or screening providers;
- from publicly available registers and records;
- from company websites;
- from professional networking services;
- from other publicly accessible internet sources;
- from commercial business-contact or marketing databases;
- from devices, vehicles or systems connected to a service; and
- from other organisations where the relevant service requires this and the disclosure is lawful.

Where information has not been obtained directly from you, we will provide the information required by data protection law unless an exemption applies or another controller is responsible for providing it.

8. Why we use personal information and our lawful bases

The lawful basis we rely upon depends upon:

- the purpose;
- the service;
- our relationship with you; and
- whether we are acting as controller or processor.

Where we act solely as processor, the Client determines the lawful basis for the underlying processing.

Where we act as controller, our purposes and lawful bases may include:

Purpose	Typical lawful basis
Providing a service purchased directly by you	Performance of or steps towards a contract
Providing and administering services for a Client	Contract with the Client, legitimate interests and/or processing as the Client's processor
Creating and administering accounts	Contract where applicable and/or legitimate interests in operating our services
Identity verification and screening	Contract, legitimate interests, legal obligations or Client instructions depending upon the service
Right to Work and regulatory checks	Legal obligation, legitimate interests or processing on behalf of the Client responsible for the check
References and background screening	Contract, legitimate interests or Client instructions, together with any additional condition required for protected information
Driver, vehicle and tachograph services	Contract, legitimate interests, legal obligations or Client instructions
Training and competency records	Contract, legitimate interests, legal obligations or Client instructions
Document-management and workforce tools	Contract, legitimate interests or Client instructions
Customer and technical support	Contract and/or legitimate interests in supporting users and operating our services
Maintaining audit trails and recording changes	Legitimate interests in accountability, accuracy, security, fraud prevention and dispute resolution, together with legal obligations where applicable
Information and system security	Legitimate interests and legal obligations
Preventing fraud and misuse	Legitimate interests and, where applicable, legal obligations
Payments, billing and accounting	Contract and legal obligations
Regulatory matters, complaints and legal claims	Legal obligations and/or legitimate interests in establishing, exercising or defending legal rights
Improving our services	Legitimate interests where appropriate; consent where required for tracking technologies
Business-to-business marketing	Legitimate interests where permitted; consent where applicable law requires it
Non-essential cookies and tracking	Consent where required

Where we rely on legitimate interests, our interests may include:

- operating and improving our business;
- providing reliable services;

- supporting users;
- protecting our systems and users;
- maintaining accurate and accountable records;
- preventing fraud;
- communicating with existing and prospective business customers;
- developing our services; and
- establishing, exercising or defending legal rights.

We consider the impact upon individuals before relying on legitimate interests.

9. What happens if information is not provided

Some information is optional.

Other information is necessary in order to:

- create or administer an account;
- verify identity;
- fulfil a Client's requested service;
- meet legal or regulatory requirements;
- submit an application;
- perform a check;
- provide a service; or
- enter into or perform a contract.

Where required information is not provided, we may be unable to provide all or part of the relevant service.

Where we act for a Client, the Client may separately require information for its own employment, compliance, contractual or legal purposes.

10. Automated processing and decision-making

Our systems use automated processing to assist in administering and delivering services.

This may include systems which:

- validate information;
- compare records;
- verify document information;
- identify missing or inconsistent information;
- perform electronic identity checks;
- calculate working or driving periods;

- identify potential tachograph infringements;
- apply rules or thresholds;
- produce reports;
- generate alerts or recommendations; and
- refer matters for human review.

At present, our own systems do not ordinarily make a final decision having a legal or similarly significant effect on an individual **solely by automated means without meaningful human involvement**.

For example, failure of an automated electronic identity check does not necessarily determine the outcome because manual or documentary verification may be available.

Where we provide information, reports or results to a Client, the Client remains responsible for employment, recruitment, disciplinary, compliance or other decisions that it makes.

We may introduce further automated processing as our services develop.

Where a service uses solely automated decision-making which has a legal or similarly significant effect on an individual, we will provide the additional information and safeguards required by law at or before the relevant processing takes place.

This may include information about:

- the nature of the automated decision;
- the information considered;
- meaningful information about the logic involved;
- the significance and likely consequences;
- the right to make representations;
- human intervention; and
- challenging the decision.

11. Who we share personal information with

Depending upon the service and our role, personal information may be shared with, or processed on our behalf by:

- the Client that requested the service;
- authorised users acting for a Client;
- the individual to whom the information relates;
- processors and sub-processors;
- subcontractors and specialist service providers;
- external digital identity, document and identity-verification providers;
- the Disclosure and Barring Service;
- the Home Office;
- the DVLA;
- police, courts, regulators and other public authorities where disclosure is lawful;
- referees and previous employers;

- qualification providers;
- professional and regulatory bodies;
- background-screening providers;
- credit, fraud, sanctions and compliance providers;
- international screening providers;
- payment providers;
- email, SMS and communications providers;
- technical and software providers;
- customer-support providers;
- hosting, backup, security and disaster-recovery providers;
- analytics and advertising providers, subject to applicable consent and cookie requirements;
- auditors;
- insurers;
- legal and professional advisers; and
- another person or organisation where disclosure is required by law or reasonably necessary to establish, exercise or defend legal rights.

Where DBS Check Limited provides a service, Aaron's Department Limited may process DBS applications on its behalf under an appropriate processing arrangement.

A current list of our material processors and sub-processors is available on request from our Data Protection Contact.

12. Information visible to Clients

Where a Client has commissioned a service, authorised users of that Client may need to see personal information about the applicant, worker, employee or driver in order to perform their responsibilities.

For example, an authorised evidence checker may need to compare information entered on an application with identity evidence.

Depending upon the service and permissions granted, authorised Client users may be able to see:

- application information;
- identity and biographical information;
- uploaded documents and evidence;
- identity-document images;
- photographs;
- check progress;
- permitted check results;
- Right to Work information;
- reference information;
- driver and tachograph information;
- training information;
- checklist responses;

- workforce or onboarding information;
- document-management information; and
- audit information relevant to the Client's use of the service.

An authorised Client user may return an application to an individual for correction, amendment or further evidence.

Where the Client is controller, its own privacy information should explain why it processes the information, who can access it and how long it retains it.

13. Client-configured information and document-management services

Some services allow Clients to configure the information or documents they require from workers, employees, applicants or other users.

Document management is a **separate service** and is not part of our DBS application system.

For example, a Client using an employee onboarding, document-management or checklist service may require an individual to upload documents which the Client considers necessary during employment or another ongoing relationship.

Where we provide storage or processing facilities upon the Client's instructions, the Client will normally determine:

- what information or documents are requested;
- why they are required;
- who can access them;
- how long they should be retained; and
- when they should be deleted.

This may result in employment, onboarding or other documents being retained throughout an individual's employment and for an appropriate period afterwards where the Client has a lawful reason to keep them.

The fact that an individual uses both a DBS service and a separate document-management service does not make documents stored in the document-management service part of the DBS application or DBS processing environment.

Clients are responsible for ensuring that information requested through configurable services is lawful, relevant, proportionate and not excessive.

Additional terms and privacy information may apply to individual services.

14. International transfers

Our core application infrastructure is hosted in the United Kingdom.

We operate our own UK data-centre infrastructure for our core services and apply technical and organisational controls appropriate to the nature of the information being processed.

Providing our services may nevertheless involve access to or processing of some personal information outside the United Kingdom.

This may include:

- overseas support and development staff;
- international screening providers;
- external identity-verification providers;
- communications providers;
- payment providers;
- analytics or advertising providers; and
- other specialist service providers.

Making personal information available remotely to a separate organisation outside the UK can constitute an international transfer even where the underlying server remains in the United Kingdom.

Where a restricted international transfer takes place, we ensure that an applicable transfer mechanism or safeguard required by UK data protection law is used.

Depending upon the recipient and destination, this may include:

- UK adequacy regulations;
- a UK International Data Transfer Agreement;
- the UK International Data Transfer Addendum to approved EU Standard Contractual Clauses;
- another safeguard permitted by applicable law; or
- a statutory exception where it is appropriate and lawful to rely upon one.

Where required, appropriate transfer assessments and additional technical or organisational safeguards are also applied.

You may contact our Data Protection Contact for further information about safeguards relating to a particular transfer.

Where the EU GDPR or another country's privacy legislation applies to a service, additional rights, notices or representative information may also apply.

14.1 Overseas support access and DBS information

We use **Aaron's Department DOOEL**, registration number **6489478**, whose registered head office is at **Apostol Guslarot 40, 1000 Skopje, North Macedonia**, to provide authorised customer-support, technical-support and software-development services.

Account information

When you create an account with us, limited account information may be made accessible to authorised members of our support and development team in North Macedonia.

This may include:

- your name;
- your email address;
- your account identifier;
- service identifiers;
- application identifiers; and
- limited information necessary to identify your account and provide support.

This enables our support team, for example, to identify the account belonging to somebody who contacts us and to provide appropriate account or technical assistance.

At first account creation, you may be asked to confirm that you have read and understood this international processing arrangement.

That confirmation records that the information has been brought to your attention. It is not intended to convert this Privacy Policy itself into a contract or to treat consent as the legal basis for every aspect of the processing.

Non-DBS services

Where you use a service other than a DBS service, authorised support or development personnel outside the UK may also be given access to personal information relating to that service where reasonably necessary to:

- provide customer or technical support;
- maintain the service;
- investigate faults;
- develop or improve the service; or
- otherwise administer it.

Access is limited according to role and to what is reasonably necessary for the relevant purpose.

DBS applications

DBS applications are subject to additional information-security and access restrictions.

Personal information contained within a DBS application is processed within the United Kingdom and is **not made available to our support or development staff in North Macedonia**.

Those staff are not provided with access to:

- personal information contained within the DBS application;
- identity documents or evidence submitted as part of the DBS application;
- DBS application documents;

- DBS result information; or
- the electronic indication of whether a certificate contains information.

Our overseas staff may continue to have access to ordinary account information, such as the account holder's name and email address, because that information forms part of the person's general account rather than the protected DBS application.

The two environments are subject to separate access restrictions.

Contacting us about a DBS application

Where support is required in relation to a DBS application, our overseas support staff use the application's **Application ID** to identify the relevant technical record without accessing the personal information contained within the DBS application.

If you contact us about a DBS application, we will ask you for your Application ID.

Please do not provide your name, date of birth, home address, identity-document information or other personal information contained in your DBS application unless an appropriately authorised UK-based member of staff specifically asks you to do so.

Our support staff should not ask you to identify a DBS application by providing your name instead of your Application ID.

If an enquiry requires somebody to view personal information contained within a DBS application, it will be referred to an appropriately authorised UK-based member of staff.

15. How long we keep personal information

We do not retain personal information for longer than is reasonably necessary for the purpose for which it is being processed, taking account of applicable legal, contractual, regulatory, audit, security and dispute-resolution requirements.

Different retention periods apply to different services.

15.1 DBS application information

Detailed DBS application information in the operational system is normally deleted **93 days after we receive the electronic DBS result** stating either:

- "Certificate contains no information"; or
- "Certificate contains information".

A limited record relating to the check may be retained for up to **three years** where reasonably necessary for audit, compliance, evidence, dispute resolution or service administration.

This retained record does not mean that we retain or have access to the contents of the applicant's DBS certificate.

15.2 Tachograph information

Tachograph and associated working-time information may ordinarily be retained for **two years** in order to support applicable road-transport and working-time requirements, subject to Client requirements and other applicable law.

15.3 Precise GPS information

Precise GPS/location information is normally retained for **93 days**, unless a longer period is reasonably necessary for a legal, contractual, investigation or dispute-related purpose.

15.4 General service information

Where no more specific retention period applies, information will generally be retained for approximately **six months** after it is no longer actively required, unless it is reasonably necessary to keep it for longer for:

- commercial purposes;
- contractual requirements;
- audit;
- complaints;
- legal claims;
- regulatory requirements; or
- another legitimate purpose.

15.5 Calls, support and communications

Call recordings, support communications, live chats and similar records are normally retained for approximately **six months**.

Relevant records may be retained for longer where necessary for:

- an audit;
- complaint;
- dispute;
- investigation; or
- legal matter.

15.6 Client-managed workforce, onboarding and document-management information

Where we act as processor for a Client, information may be retained for the period specified by that Client.

This can include documents retained throughout an individual's employment or other relationship with the Client where the Client has a lawful reason to keep them.

15.7 Training and certification information

Training and certification information may be retained for as long as reasonably necessary to evidence:

- attendance;
- completion;
- certification;
- competence; or
- compliance,

or for the period instructed by a Client where we act as its processor.

15.8 Financial information

Transaction, accounting and tax information may be retained for periods required by applicable legal, taxation and accounting obligations.

15.9 Marketing suppression information

Where somebody objects to direct marketing, we may retain the minimum information necessary to ensure that their objection continues to be honoured.

Retention of a suppression record is not continued marketing.

15.10 Legal holds and exceptional retention

Information may be retained beyond the normal period where reasonably necessary for:

- litigation;
- legal claims;
- complaints;
- investigations;
- regulatory requirements;
- law-enforcement requests; or
- another legal obligation.

15.11 Backups and disaster recovery

Backup and disaster-recovery systems operate separately from normal live information.

Routine backups are maintained in accordance with our backup cycle and selected monthly disaster-recovery copies may be retained for up to **three years**.

As a result, information deleted from our live operational systems may continue to exist within a protected backup until that backup reaches the end of its retention period.

Information contained solely within these backups is not available for ordinary operational use and is not routinely searched or restored to retrieve individual records.

It is retained for disaster recovery, resilience and system-recovery purposes.

If a backup is restored following an incident, applicable current deletion, retention and marketing-suppression controls will be reapplied as part of the recovery process.

16. Information security

We use technical and organisational measures designed to protect personal information from:

- unauthorised access;
- unlawful processing;
- accidental loss;
- destruction;
- alteration; and
- inappropriate disclosure.

Measures are selected according to the nature and sensitivity of the information and may include:

- role-based access controls;
- authentication controls;
- encryption;
- system and network security;
- segregation of access;
- audit logging;
- security monitoring;
- secure development practices;
- backup and disaster-recovery controls;
- data minimisation;
- staff confidentiality requirements;
- training;
- supplier controls; and
- independent security assessment.

Services involving DBS information are operated subject to the security, information-assurance and access-control requirements applicable to our roles as a **DBS Registered Body and Umbrella Body, a Responsible Organisation for Basic DBS checks and a DBS e-Broker**, including applicable DBS processing requirements and required independent security testing.

No electronic system can guarantee absolute security, but we regularly review our safeguards in light of the information being processed and the risks involved.

17. Cookies and similar technologies

Our websites may use cookies and similar technologies for purposes including:

- essential website functionality;
- security;
- remembering preferences;
- analytics;

- service improvement;
- advertising measurement;
- advertising;
- embedded content; and
- communication or support functions.

The technologies used vary between our websites.

Non-essential cookies and similar technologies will not be placed before consent where consent is required by law.

Where consent is requested, users should be able to reject non-essential technologies as easily as they can accept them.

Strictly necessary technologies, and other technologies falling within an applicable statutory exemption, may be used without consent where permitted by law.

Details of the technologies used on a particular website, their providers, purposes and applicable retention information are provided through that website's separate **Cookie Policy** and cookie controls.

18. Direct marketing

We market our services to organisations and business contacts.

This may include:

- companies;
- public bodies;
- charities;
- partnerships;
- sole traders; and
- other organisations.

Marketing information may come from:

- existing customer relationships;
- enquiries;
- publicly available business information;
- company websites;
- professional networking services;
- directories;
- commercial business-contact databases; and
- other lawful sources.

We may hold information concerning named employees, directors, owners or other business contacts where relevant to communicating with an organisation.

We may contact business recipients by:

- email;
- telephone;
- SMS; or
- post,

where permitted by applicable law.

We rely on legitimate interests for business-to-business marketing where appropriate and use consent where PECR or another applicable law requires it.

You have an **absolute right to object to direct marketing at any time**.

You can object by:

- using the unsubscribe mechanism provided in a marketing communication; or
- contacting our Data Protection Contact.

Opting out of marketing does not prevent us from sending communications necessary to administer an existing account, service or contractual relationship.

We may retain limited information on a suppression list so that your marketing preference continues to be honoured.

19. Your data protection rights

Depending upon the circumstances, applicable data protection law may provide rights including:

- the right to be informed about how personal information is used;
- the right to access personal information;
- the right to correct inaccurate or incomplete information;
- the right to request deletion;
- the right to restrict processing;
- the right to object to processing;
- the right to data portability in applicable circumstances;
- the right to withdraw consent where processing genuinely relies upon consent; and
- rights and safeguards relating to qualifying solely automated decisions.

These rights are not absolute and some apply only in particular circumstances.

19.1 Where we act as processor

If the information is controlled by your employer, prospective employer or another Client, that organisation will normally be responsible for responding to your request.

You may contact it directly.

If you send the request to us, we may need to pass it to the relevant Client and will provide reasonable assistance to the Client in fulfilling its obligations.

19.2 Where we act as controller

You can exercise your rights by contacting our Data Protection Contact.

You do not have to use a particular form or use particular wording.

We may request information reasonably necessary to establish your identity before disclosing personal information or carrying out certain requests.

We normally respond to applicable rights requests within one month, subject to the extensions, clarification provisions and other rules permitted by data protection law.

There is normally no charge, although the law permits organisations to charge a reasonable fee or refuse a request in certain limited circumstances.

20. Changing and correcting information

Where the service permits it, you may be able to update your own personal information through your account.

Changes may be recorded in an audit history showing matters such as:

- the previous information;
- the revised information;
- when the change was made; and
- who made the change.

Where an application is being processed for a Client, an authorised evidence checker, countersignatory or other Client user may return an application to the applicant for correction, amendment or further evidence.

Updated information may be visible to the Client where relevant to the service it commissioned.

21. People aged 16 or 17

Some of our services may legitimately involve people aged 16 or 17.

For example, certain DBS checks and driver-related services may apply from age 16.

A person aged 16 or 17 may create and use an account in the same manner as an adult where the relevant service permits this.

We recognise that privacy information provided to younger users must remain clear and understandable and will provide additional explanations where appropriate.

Our services are not intended to encourage unnecessary collection of information relating to children.

22. Links and independent third parties

Our websites and services may contain links to websites or services operated by other organisations.

Where another organisation independently determines why and how it processes information, its own privacy information will apply to that processing.

We are not responsible for the independent processing activities of another controller.

This does not affect our responsibilities for organisations which process personal information on our behalf.

23. Data protection complaints

If you are concerned about the way we have processed your personal information, please contact our Data Protection Contact.

We maintain a procedure for handling data protection complaints.

We will:

- provide an accessible means of making a complaint;
- acknowledge a data protection complaint within the period required by law;
- take appropriate steps to investigate the complaint;
- keep the complainant appropriately informed; and
- communicate the outcome without undue delay.

Under current UK law, a data protection complaint must be acknowledged within **30 days**.

You also have the right to complain to the **Information Commissioner's Office (ICO)**.

Information about making a complaint is available from the ICO.

Where another country's data protection legislation applies, you may additionally have the right to complain to the competent supervisory or regulatory authority in that jurisdiction.

24. Changes to this Privacy Policy

We may update this Privacy Policy where:

- applicable law changes;
- regulatory guidance changes;
- our services develop;
- our processing activities change;
- our suppliers or processing arrangements materially change; or
- additional information is required to explain our processing more clearly.

The introduction of a new service does not necessarily require this Privacy Policy to be rewritten where the new service falls within the purposes, data categories and types of processing already described.

Where a new service involves:

- a materially different purpose;
- materially different sensitive processing;
- significant solely automated decision-making; or
- another processing activity which individuals would reasonably expect to be specifically explained,

we will provide appropriate additional information, which may take the form of an update to this Privacy Policy or a supplementary privacy notice presented in connection with that service.

Where a material change affects existing users, we may notify affected users by:

- email;
- an account notification;
- an in-application message;
- notification through the relevant Client; or
- another appropriate method.

Continued use of a service will not by itself be treated as consent where consent is legally required.

The date at the beginning of this Privacy Policy identifies the current version.

25. Contact us

For questions concerning this Privacy Policy, exercising your rights, making a data protection complaint, requesting our processor/sub-processor information, or asking about international-transfer safeguards, please contact:

Data Protection Contact:

data-protection@aaronsdepartment.com

Legal entity:

Aaron's Department

Registered office:

43 Church Lane, Pudsey, LS28 7RR

Where we process your information solely on behalf of a Client, you may also contact that Client directly about the purposes for which it processes your information.