Product Schedule

Identity and Fraud Services

V1.1 effective from 1 October 2025

Table of contents

Part 1– Identity and Fraud Services general terms

Part 1 applies to all Identity and Fraud Services

1 What is this document?

1.1 It applies to Identity and Fraud Services

This Product Schedule only applies to Identity and Fraud Services. All references to Services in this Product Schedule refer to Identity and Fraud Services.

1.2 Definitions

Capitalised terms used in this Product Schedule have the meaning given to them in the Work Order, or the Experian Dictionary, accessible at www.experian.com.au/terms.

2 How do we provide the Services?

2.1 We operate under applicable Laws

Our ability to provide the Services is subject to Law (including Privacy Laws).

2.2 We rely on Third Parties

When providing our Services, we rely on information provided to us by Third Parties (e.g. Third Party Data providers) and we and our Related Bodies Corporate may record and disclose your use of the Services to relevant Third Parties.

3 What are your obligations?

3.1 Before using the Services

Before using the Services, you must obtain all necessary consents and issue all notices and disclosures required under Appendix A and applicable Laws, including Privacy Laws, to provide or receive information about a person.

You must keep records of these and share them with us on request.

3.2 Using the Services

You must:

a. only use the Service for the Authorised Use (including under Appendix A) and in line with their intended purpose and applicable Laws;
b. implement and maintain industry best practice security measures and safeguards in relation to your computer systems, network and internet connectivity to access the Services;
c. comply with all technical safeguards and access restrictions designed to protect the integrity and security of the Services;
d. keep all Credentials secure and confidential. If there is any unauthorised use of Credentials, you must promptly notify us, change the affected Credentials (if you can), and follow our reasonable instructions;

e. protect the Services from unauthorised access, use, modification, reproduction, publication, or distribution, including through reverse engineering, automated tools or processes, or harmful code;
f. ensure that the Services or Experian Data are not resupplied, resold, or repackaged;
g. restrict access to the Services to you, your Authorised Users and Authorised Third Parties only; and
h. only use the Services on hardware, networks, systems and software that meet any minimum specifications notified by us from time to time.

Unless required by Law, you must not voluntarily produce any Experian Data in legal proceedings or identify us, our Related Bodies Corporate, the Services, or our Confidential Information as a source of reference.

3.3 You are responsible for Authorised Users

a. If Authorised Users access the Services, you:
   i. must maintain a list of Authorised Users and share it with us on request;
   ii. must ensure that your Authorised Users comply with the Agreement and our reasonable directions to use the Services;
   iii. are responsible for your Authorised Users' use of the Services; and
   iv. acknowledge that we may disable Authorised Users that are deemed inactive or we reasonably suspect have breached the Agreement.
b. If an Authorised User no longer needs access to the Services, you must remove their access. Anyone with access will be considered authorised by you.
c. We may monitor your Authorised Users use of the Service to ensure your compliance with the Agreement, our security standards and to prevent fraud and unauthorised use. You are responsible for obtaining any necessary consents from your Personnel and Authorised Users in relation to this clause.

3.4 You are responsible for how you use the Services

The Services aren't designed or intended to be relied upon as the sole basis for any business decision. You are solely responsible for any decisions made (or not made) by you or your Authorised Users in relation to the use of the Services.

4 How do we manage intellectual property?

4.1 Ownership and licensing of Existing IP

You and we each own and continue to own all of our respective Existing IP. If any of your Existing IP forms part of any of our Services, you grant us a non-exclusive, perpetual, irrevocable, royalty-free licence to use and modify that Existing IP to the extent required to deliver the Experian Services.

4.2 We, our licensors and Third Party Data providers keep our IP

We (or our licensors) own all right, title, and interest, including IP Rights, in the Services at all times. We don't, at any time, transfer any ownership rights in the Services and we reserve all rights not expressly granted.

Where the Services include Third Party Data, our Third Party Data providers retain all rights, title and interest (including IP Rights) in the Third Party Data.

4.3 IP created during Service provision

All right, title and interest, including IP Rights, in any Enhancements or Joint IP vests in us on creation. If you acquire any IP Rights in any of our Services, Enhancements, or Joint IP, you:

a. assign those IP Rights to us (or our licensor) with effect from acquisition; and
b. agree to do all things reasonably required by us to give effect to such assignment.

Part 2 – Service-specific terms

Each set of service specific terms applies only to the Service of the same name (or as otherwise set out below)

5 Identity Verification Services terms

5.1 Service provision

The Services are provided by Experian Australia Operations Pty Ltd under a joint venture arrangement with GBG ANZ Pty Ltd (**GBG**).

5.2 Data management and record keeping

a. The outputs of the Service, including any reports and match result (**Results**) won't contain any Personal Information except for what was provided to us as part of the verification request.

b. Subject to clause 5.2 d., identity verification records (including Client Data and Results) (**Verification Records**) are kept by the Service for a period you choose (up to a maximum of 7 years), with a default period of 12 months (**Retention Period**).

c. Regardless of the Retention Period, any Personal Information in retained Verification Records will be de-identified after 12 months, unless you ask us to de-identify sooner.

d. Upon de-identification, only information needed for billing (including the unique reference ID for a verification) will be kept by the Service. This will be kept for the longer of our regulatory requirements or until you ask us to delete it (after all related billing is settled). You are responsible for keeping the unique reference ID so you can match it to the Results after deletion.

e. The Services don't and aren't intended to operate as a record management system. You are responsible for having your own systems and controls in place to manage your identity verification records.

f. All retained Verification Records will be deleted within 30 days after the Agreement ends.

g. If you use single sign-on (SSO), we'll need to share your users' work email addresses with GBG and/or its third-party providers. This includes transferring that information to the United Kingdom. You agree to this transfer and understand that the information may be stored and processed outside Australia, in line with applicable privacy laws.

5.3 Third Party Data

a. Third Party Data providers may retain a copy of any Client Data you provide as required for legal, regulatory, compliance, auditing, insurance and/or record keeping purposes.

b. We're unable to make requests for changes, updates, or deletions to the Third Party Data provider's databases, as they manage and maintain those databases independently.

c. To use the Australian Document Verification Service (**DVS**) or New Zealand Department of Internal Affairs (**DIA**) data sources, we need approval from DVS or DIA for us to enable the data source for your use.

5.4 Third Party Terms

If you access the below Third Party Data sources, you agree to, and must comply with the applicable Third Party Terms:

Data source	Third Party Terms
DVS	DVS Business User Terms and Conditions of Use available on the www.idmatch.gov.au website.
Superannuation & Payroll	Superannuation & Payroll Data Source Terms and Conditions which you can access at www.experian.com.au/terms#additional.
ConnectID	ConnectID Data Source Terms and Conditions, which you can access at www.experian.com.au/terms#additional.
Australian Death Check	Australian Death Check User Terms and Conditions, which you can access at www.experian.com.au/terms#additional.

6 greenID Trust Alerts service terms

6.1 Identity Verification Services service terms apply

Section 5 of this Product Schedule (Identity Verification Services also applies to the greenID Trust Alerts Service.

6.2 Additional service terms

You must comply with the greenID Trust Alerts service-terms, which you can access at www.experian.com.au/terms#additional.

7 Biometric Services terms

7.1 GBG Biometric Services terms

Experian Australia Operations Pty Ltd is an authorised reseller of GBG's biometrics services and software products.

By using the GBG Biometric Service, you agree to comply with the GBG Biometric Services Terms & Conditions, which you can access at www.experian.com.au/terms#additional.

7.2 IDVerse Biometric Services terms

Experian Australia Operations Pty Ltd (in Australia) and Experian Operations New Zealand Limited (in NZ) are authorised resellers of IDVerse biometrics services and software products.

a. By using the IDVerse Biometric Service, you agree that you are entering into the applicable end user licence agreement (**EULA**) set out below with OCR Labs Pty Ltd (referred to in this section as **IDVerse**):

IDVerse EULA type	Link to EULA
EULA for a 'small business' as defined under the Australia Consumer Law	The IDVerse Small Business EULA, accessible at www.experian.com.au/terms#additional.
EULA for all other Clients	The IDVerse End User Licence Agreement, accessible at www.experian.com.au/terms#additional.

b. The end user consent screen must include a link to your privacy policy and explain how IDVerse process Personal Information. Any changes to the end user consent screen require IDVerse's written permission.

c. IDVerse may, at its discretion, retire older versions of the Service and mark them as "end of life." If this happens, we'll give you at least 9 months' notice. During that time, you must upgrade to at least the second newest version. After the end-of-life date, IDVerse may stop hosting or supporting the retired version.

d. IDVerse may require you to include specific wording in the consents and notices required for end users, to help meet its legal obligations. You must comply with IDVerse's instructions in relation to this.

e. If you use the IDVerse fraud hub 'blocklist' functionality, you must not add the image or identity document of a person you know or reasonably suspect is a victim of identity fraud to your blocklist.

f. Neither we or IDVerse make any warranties that the suitability of Services meet your legal or privacy obligations.

8 PEP and Sanctions Services terms

8.1 ComplyAdvantage PEP and Sanctions Service additional terms

a. The Services are provided by Experian Australia Operations Pty Ltd under a joint venture arrangement with GBG ANZ Pty Ltd (GBG).

b. By using this Service, you agree to comply with the ComplyAdvantage Services Terms, which you can access at www.experian.com.au/terms#additional.

8.2 Acuris PEP and Sanctions Service terms

a. Experian Australia Operations Pty Ltd provides the Services under a reseller arrangement with Consulting (Singapore) Pte Ltd trading as Acuris Risk Intelligence (**Acuris**). Acuris is a Third Party Data provider.

b. You must not remove any copyright or other notice included in any information or documentation provided to you under this Service.

9 Deceased Wash service terms

9.1 Service provision

Experian Australia Operations Pty Ltd provides the Service as an approved data service broker for the Australian Death Check.

9.2 Using the Service

a. We can only provide the Services if you apply to the Queensland Registry of Births, Deaths and Marriages (as the Australian Coordinating Registry) for ADC data access, and your application is approved.

b. By using the Service, you agree to comply with the ADC User Terms and Conditions, which you can access at www.experian.com.au/terms#additional.

Appendix A

Authorised Uses, notification and consent requirements

Data source / Service	Authorised Use	Notifications you must provide to a person	Consents and/or acknowledgements you must obtain from a person (in writing)
All data sources	For your lawful internal business purposes.	You must explain the purpose of the identity check and what information will be collected, so the person can decide whether to allow access to their personal information.	The person must agree that you can authorise Experian, its related companies, and third-party providers to collect, use, store, and share their personal information for identity verification and (if applicable) fraud prevention.
DVS data source (AU)	In accordance with the DVS Business User Terms and Conditions of Use and applicable Laws.	In accordance with the DVS Business User Terms and Conditions of Use and applicable Laws.	In accordance with the DVS Business User Terms and Conditions of Use and applicable Laws.
DIA data source (NZ)	For identity verification purposes only, in accordance with applicable Laws.	You must explain the purpose of the identity check and what information will be collected, so the person can decide whether to allow access to their personal information.	The person must provide express consent for you to authorise Experian, its related companies, and third-party providers to collect, use, store, and share their personal information for identity verification purposes.
Credit header data source (AU)	To assist you in meeting your identity verification obligations under the AML/CTF Act.	As set out in section 35A(2) of the AML/CTF Act. If you're unable to verify the identity of a person using this data source, you must also comply with your notification obligations under section 35C(2) of the AML/CTF Act.	As set out in section 35A(2) of the AML/CTF Act.
Credit header data source (NZ)	To assist you in meeting your identity verification obligations under the AML/CFT Act.	As required under the AML/CFT Act, Privacy Laws and any other applicable Laws.	As required under the AML/CFT Act, Privacy Laws and any other applicable Laws.
ConnectID data source	For identity verification purposes only, in accordance with applicable Laws.	As set out in clause 6.1 of the ConnectID data source terms, accessible at www.experian.com.au/terms#additional.	As set out in clauses 2.3 and 6.1 of the ConnectID data source terms, accessible at www.experian.com.au/terms#additional.
NZ Transport Agency data	For verifying the existence and currency of a drivers licence record only (for identity verification purposes), in accordance with applicable Laws.	You must explain the purpose of the drivers licence verification and what information will be collected, so the person can decide whether to allow access to their personal information.	The drivers licence holder must provide express consent for you to authorise Experian, its related companies, and third-party providers to collect, use, store, and share their personal information for identity verification purposes.
ComplyAdvantage PEP and Sanctions Service	As set out in clause 1 of the ComplyAdvantage Services Terms, accessible at www.experian.com.au/terms#additional.	As required under Privacy Laws and any other applicable Laws.	As set out in clause 3.1(c) of the ComplyAdvantage Services Terms, accessible at www.experian.com.au/terms#additional.
Acuris PEP and Sanctions Service	For your lawful internal business purposes.	As required under Privacy Laws and any other applicable Laws.	As required under Privacy Laws and any other applicable Laws.

Superannuation and payroll data source	For identity verification purposes only, in accordance with applicable Laws.	As required under Privacy Laws and any other applicable Laws.	As set out in clauses 3 and 4 of the Superannuation and payroll data source terms, accessible at www.experian.com.au/terms#additional.
GBG Biometric Services	For identity verification purposes only, in accordance with applicable Laws.	As required under Privacy Laws and any other applicable Laws.	As required under Privacy Laws and any other applicable Laws.
IDVerse Biometric Services	For identity verification purposes only, in accordance with applicable Laws.	As required under Privacy Laws and any other applicable Laws.	As required under Privacy Laws and any other applicable Laws.
Australian Death Check data source	For your lawful internal business purposes, in accordance with applicable Laws and the Australia Death Check terms, accessible at www.experian.com.au/terms#additional.	As required under Privacy Laws and any other applicable Laws.	As required under Privacy Laws and any other applicable Laws.