Experian's Identity & Fraud ('ID&F') business function helps lenders and other businesses and organisations by verifying information to help them make more accurate and faster decisions, on matters such as identity and eligibility. ID&F also operates as a Fraud Prevention Agency (FPA) which collects, maintains and shares, data on confirmed and suspected fraudulent and financial crime activity. This document describes how Experian uses and shares personal data within its ID&F business.

This document answers these questions:

1. What does Experian's ID&F business use personal data for?
2. What are Experian's legal grounds for handling personal data in relation to its ID&F business?
3. What kinds of personal data does Experian's ID&F business use, and where does it get it?
4. Who does Experian share personal data with?
5. Where is personal data stored and sent?
6. For how long is personal data retained?
7. Does Experian's ID&F business make decisions about consumers?
8. What can I do if I want to see the personal data held about me?
9. What can I do if my personal data is wrong?
10. Can I object to the use of my personal data and have it deleted?
11. Can I restrict what Experian does with my personal data?
12. Who can I complain to if I'm unhappy about the use of my personal data?
13. Where can I find out more?

1. What does Experian's ID&F business use personal data for?

Experian's ID&F business provides services that are used to:

- verify identities and other personal details
- detect and prevent fraud
- detect and prevent financial crime
- detect and prevent money laundering.

Experian provide services in all of the areas listed above.

As part of providing these services, Experian may process personal data about you.

Details of the personal data that can be processed includes (but is not limited to):

- Name
- Date of Birth
- Address and Previous Address History
- Telephone Number(s) including Mobile
- Email Address
- Other Contact Details
- Fraud indicators and fraud outcomes
- Online transactions, logins, purchases and quotations.
- Employment Details
- Financial Associates
- Credit and Financial Information
- Device identifiers (including IP Address, device type, make, model)
- Cookie's data
- Search footprints (including identity and fraud searches requested through our software)
- Document identifiers (including Driving Licence, Passport reference numbers or National IDs where issued)
- Vehicle Details
- Facial images provided by you as part of the identity and fraud verification journey
- Behavioural characteristics (such as information on how you interact with any devices you use to access products or services)
- Leaked data made available on the 'dark web'

- Public information (e.g. adverse media, social media profiles & activity, politically exposed persons and sanctions information)

This personal data is used to:

(a) Validate that an identity exists and verify that an individual presenting an identity is the true owner of that identity;

This may include accessing the Experian credit bureau, as well as other data sources within Experian or from other data suppliers, to compare the personal data that you supply with existing records to confirm that your identity exists and that you are the owner of that identity.

If there is no evidence of your identity or there are inconsistencies with the data that you supply with the data that we hold, then we may tell our client that we are unable to verify your identity and you may be asked to prove your identity through other means, such as the provision of identity documents.

(b) Verifying that information, such as age, residency, address history, financial details and income, supplied by consumers is accurate

If the data that you supply will have a material effect on whether you will be provided with goods or services or the ongoing servicing of any account and is suspected of being incorrect based on the information that we hold, then we will advise our client of any discrepancies. They will use this information, and the results of any subsequent investigations they undertake, to determine whether they still wish to provide those goods or services to you or allow you to operate an account with them.

(c) Detecting and preventing criminal activity, fraud and money laundering

The information you supply will be checked against records of confirmed or suspected criminal activity, fraud or money laundering and if a connection is found then we will make our clients aware of this. They will use this information, and the results of any subsequent investigations they undertake, in order to decide on whether they still wish to provide goods or services to you or continue to allow you to operate an account with them.

(d) Profiling, statistical analysis and analytics in the area of fraud detection and prevention

The data that you supply may be aggregated with data from other consumers in order to generate statistics or profiles that will be used by our clients to help them predict the likely fraud risk associated with certain characteristics. This will help our clients make decisions about your request for goods or services and inform any investigation into your application or your existing account.

(e) New product development, testing and research

The data that you supply will be used to help develop new products, services and technologies to improve the prevention and detection of fraud, money laundering and other criminal activity.

(f) Other purposes where you have given your consent or where required/permitted by law

2. What are Experian's legal grounds for handling personal data in relation to its ID&F business?

The UK's data protection laws allow the use of personal data where its purpose is legitimate and isn't outweighed by the interests, fundamental rights or freedoms of data subjects. The law calls this the Legitimate Interests condition for personal data processing. The Legitimate Interests being pursued by Experian's ID&F business are:

(a) Verifying identity and eligibility
(b) Detecting and preventing financial crime, fraud and money laundering
(c) Supporting compliance with legal and regulatory requirements

Interest	Explanation
Verifying identity and eligibility	Providing electronic identity verification and eligibility services to our clients allows a person to have prompt access to goods and services without the inconvenience of providing documentation that they would otherwise be forced to provide. This means that the organisation they are dealing with can comply with legal and regulatory obligations, including Anti-Money Laundering regulations and the sale of age-restricted goods. This activity benefits individuals as it protects them from having their details used to open accounts in their name and thus becoming a victim of fraud themselves. It is in the legitimate interest of our clients to be able to have confidence that they are dealing with the genuine person and not a fraudster pretending to be that person.
Detecting and preventing financial crime, fraud and money laundering	Prevention and detection of financial crime, fraud and money laundering and other criminal activity is in the legitimate interest of the fraud prevention agencies and their clients. In cases where the fraud involves identity theft then it is beneficial to the individual and therefore also in their interest. It is also to the benefit of wider society and therefore in the public interest.
Supporting compliance with legal and regulatory requirements	ID&F services may be used by organisations to help them comply with their own regulatory obligations, for example, complying with anti-money laundering obligations and regulations set by the FCA. This is in the legitimate interest of our clients. Further, these regulatory obligations are in place in the interests of wider society, so facilitating compliance with them indirectly benefits society as a whole, which is in the public interest.

The use of personal data is subject to an extensive framework of safeguards that balance the legitimate interests set out above with the fundamental rights and freedoms of the people whose data is used and shared. The framework includes information given to people about how their personal data will be used and how they can exercise their rights to obtain their personal data, have it corrected, erased or restricted, object to it being processed, and complain if they are dissatisfied. It also includes extensive due diligence checks on clients, robust contractual arrangements and internal data management processes. These safeguards help sustain a fair and appropriate balance and to protect the rights and freedoms of individuals.

Legal obligations

In some circumstances we are required by law to use or share personal data in particular ways. This happens, for example, when a court, law enforcement agency or regulator makes a legally binding request or order for disclosure of personal data. It also happens if you chose to exercise your rights, for example by requesting a copy of your own personal data from us.

3. What kinds of personal data does Experian's ID&F use, and where does it get it?

Experian's ID&F business obtains and uses information from different sources, so it often holds different information and personal data from each other. However, most of the personal data they do hold falls into the categories outlined below;

(a) Client-provided data associated with applications, transactions and existing accounts
(b) Data provided via fraud prevention schemes, such as Cifas and National Hunter
(c) Credit Bureau data
(d) Other Experian business functions
(e) Data from third parties
(f) Information available online
(g) Data derived from the sources above
(h) Scores
(i) Statistical data derived from the data referenced above

Information Type	**Description**	**Source**
Client-provided data associated with applications and existing accounts	As part of using our ID&F services, clients submit data on applications and existing accounts for checking. These records, which include details of the individuals, associated with these applications or accounts are retained in order to be used for future validation. In addition to this information, we may also receive and retain business data including name, address and details of shareholders and directors.	This data is submitted by Clients as part of their use of our ID&F services. It may also include transactions, logins, purchases and quotations.
Data provided via fraud prevention schemes, such as Cifas and National Hunter	Experian are members of Cifas, another fraud prevention agency, and receive data relating to confirmed fraud cases from them, which are made available within our ID&F services. Experian are also the service provider for the National Hunter service, which is administered by N Hunter Limited. This service includes both confirmed fraud cases and previous application records.	Cifas data is received directly from Cifas (www.cifas.org.uk) National Hunter data is received directly from the National Hunter members themselves (www.nhunter.co.uk)
Credit Bureau data	Experian's credit bureau, including search footprints, credit account details, electoral register, are all used as part of ID&F services.	Details of the sources of the Credit Bureau data are available through the following notice: https://www.experian.co.uk/legal/crain/

Data from other Experian business functions	Contact data you provide when signing up to Experian's free or paid for accounts ('Free Account' and 'Credit Expert') and data collected by Experian's marketing services business is used in ID&F services.	Contact data is received from Experian's Consumer Services business and is only used for the reasons explained in the Consumer Privacy Policy - https://www.experian.co.uk/consumer/privacy.html. Marketing data is received from Experian Marketing Services. The Consumer Information Portal provides information on how Experian collects, uses and shares personal data for its clients' marketing purposes and other related activities.
Data from third parties	This data is provided by both private and public sector entities and includes name, address, telephone, email, IP and other device data, fraud outcomes, sanctions and politically exposed person (PEP) data, adverse media and mortality data.	Experian receive this data from reputable commercial sources under contracts agreed from time to time.
Information available online	Personal data that has been leaked by criminals on to the dark web or publicly made available by individuals or companies on social media and collected by a third party or Experian.	Social media platforms and other publicly available websites that permit data scraping by third parties. Data that has been leaked onto the dark web is located and shared by CSIdentity, an Experian group company. See privacy policy here for more details.
Data derived from the sources above	Combinations of the data referenced above may be used in order to derive high fraud risk datasets, such as high risk geographical areas.	These datasets are derived from the other data referenced in this table.
Scores	Identity scores are created to indicate the strength of identity information associated with an individual. Fraud risk scores are created to indicate the probability of fraud associated with an application, transaction or an existing account.	These scores are generated using algorithms and techniques such as scorecards and machine learning methods.

Statistical data derived from the data referenced above	Aggregated statistical data such as velocity (for example, the number of times an individual has applied within a specified time period) and combination statistics (for example, the number of times an individual has applied with a specific email address)	These statistics would be based on Client supplied application data and/or search footprints from credit bureau data and data from third parties.

4. Who does Experian share personal data with?

(a) Clients using our ID&F services

Experian supply their ID&F products and services in various sectors, such as (but not limited to) banks, financial services companies, building societies, utility companies, insurance companies, gaming companies, retailers and mobile phone companies.

(b) Fraud Prevention Agencies and Third-Party ID&F Solution Providers

Although, Experian's ID&F business is a Fraud Prevention Agency in its own right, Experian Consumer Services business also shares data with other recognised Fraud Prevention Agencies, such as Cifas and National Hunter.

Experian also enables our clients to access ID&F data and solutions provided by other providers so we will share personal data with those providers for the purposes of new product development and where our clients instruct us to do so.

(b) Resellers, distributors and agents

Organisations that package and resell ID&F services to other organisations. Those organisations are the same types of ones as referenced under (a)

(d) Public bodies, law enforcement and regulators

Some public bodies and law enforcement organisations use some of Experian's ID&F services as clients. Experian may get requests for information under

(e) Processors, where Experian uses other organisations to perform tasks on their behalf (for example, IT service providers and call centre providers)

(f) Individuals (People are entitled to obtain copies of the personal data Experian hold about them. You can find out how to do this below.)

5. Where is personal data stored and sent?

Experian is based in the UK, which is where our main databases are. We have operations elsewhere inside and outside the European Economic Area, and personal data may be accessed from those locations too. In both cases, the personal data used in those locations is protected by UK and European data protection standards.

Sometimes we will need to send or allow access to personal data from elsewhere in the world. This might be the case, for example, when one of our processors or a client is based overseas or uses overseas data centres.

While the UK and countries in the European Economic Area all ensure a high standard of data protection law, some parts of the world may not provide the same level of legal protection when it comes to personal data. As a result, when we do send personal data overseas we will make sure suitable safeguards are in place in accordance with UK data protection requirements, to protect the data. For example, these safeguards might include:

- Sending the data to a country that's been approved by UK authorities as having a suitably high standard of data protection law. Examples include the Isle of Man, Switzerland and Canada
- Putting in place a contract with the recipient containing terms approved by UK authorities as providing a suitable level of protection
- Sending the data to an organisation which is a member of a scheme that's been approved by UK authorities as providing a suitable level of protection.

If your data has been sent overseas like this, you can find out more about the safeguards used by contacting us as follows:

By Post: Experian, PO BOX 9000, Nottingham, NG80 7WF
Web Address: http://www.experian.co.uk/consumer/contact-us/index.html

Email: uk.dpo@experian.com.

6. For how long is personal data retained?

Identifiers

Identification data like names and addresses are kept while there's a continuing need to keep it. This need will be assessed on a regular basis, and data that's no longer needed for any purpose will be disposed of.

Search footprints

Experian keeps most search footprints for one year from the date of the search, although it keeps debt collection searches for up to two years. Client ID&F search footprints are typically stored for 13 months but it may vary depending on individual client configurations.

Fraud Data

Records that have been confirmed as relating to fraudulent applications or accounts are retained for up to 6 years since the time of update.

Other data

Other third party supplied data such as client provided applications data, politically exposed persons (PEPs) and sanctions data and mortality data will be stored for a period determined by criteria such as the agreed contractual terms.

Archived data

Experian may hold data in an archived form for longer than the periods described above, for things like research and development, analytics and analysis, (including refining lending and fraud strategies, scorecard development and other analysis such as loss forecasting), for audit purposes, and as appropriate for establishment, exercise or defence or legal claims. The criteria used to determine the storage period will include the legal limitation of liability period, agreed contractual provisions, applicable regulatory requirements and industry standards.

7. Does Experian's ID&F business make decisions about consumers?

Experian's ID&F business does not make decisions or tell organisations what decisions to make about consumers. It is for each organisation to decide on whether to accept or decline an application or continue to service an account based on their own risk assessment and investigations. Our ID&F business provides organisations with services that reflect the level of fraud or ID risk and the organisation decides how that information is used. An organisation's own data, knowledge, processes and practices will play the most significant role in those decisions

Our ID&F services may provide similar information to our clients, but those service may lead to different decisions because (i) each client may place differing importance on some information compared to others (ii) each client may take into account information available to it from other sources. These are some reasons why a person may receive a "yes" from one lender but a "no" from another.

8. What can I do if I want to see the personal data held about me?

Data access right

You have a right to find out what personal data Experian holds about you including the IDF business. Experian provides more information about access rights on its website.

To get online information: http://www.experian.co.uk/consumer/contact-us/index.html

To make a request by post: Customer Support Centre, Experian Ltd, PO BOX 9000, Nottingham, NG80 7WF

9. What can I do if my personal data is wrong?

When Experian receives personal data, we perform lots of checks on it to try and detect any effects or mistakes. Ultimately, though, we rely on the suppliers to provide accurate data. If you think that any personal data we hold about you is wrong or incomplete, you have the right to challenge it. It's worth knowing that we won't have the right to change the data without permission from the organisation that supplied it, so we will need to take reasonable steps to check the data first, such as asking the organisation that supplied it to check and confirm its accuracy. If the data does turn out to be wrong, we will update our records accordingly.

If the data is relating to a record on the credit bureau and we still believe it to be correct after completing our checks, we'll continue to hold and keep it - although you can ask for a note to be added to your file indicating that you disagree or provide an explanation of the circumstances. If you'd like to do this, you should contact us using the contact details in section 8 above.

10. Can I object to the use of my personal data and have it deleted?

This section helps you understand how to use your data protection rights to object to your personal data being used and how to ask for it to be deleted. To understand these rights and how they apply, it's important to know that Experian's ID&F business holds and processes personal data under the Legitimate Interests ground for processing (see section 2 above for more information about this), and doesn't rely on consent for this processing. You have the right to lodge an objection about the processing of your personal data. If you want to do this, you should contact us using the contact details set out in section 6 above. Whilst you have complete freedom to contact us with your objection at any time, you should know that under the General Data Protection Regulation, your right to object doesn't automatically lead to a requirement for processing to stop, or for personal data to be deleted, in all cases.

Please note that because of the importance of identity verification and fraud prevention to the UK's financial system, and the important purposes the personal data is needed for (confirming eligibility and preventing fraud, financial crime and money laundering) it will be very rare that we do not have compelling, overriding grounds to carry on using the personal data following an objection. In many cases, it won't be appropriate for us to restrict or to stop processing or delete personal data, for example, where the result would be to hide previous fraudulent activity that could enable a person or organisation to get credit they otherwise wouldn't be eligible for.

11. Can I restrict what Experian does with my personal data?

In some circumstances, you can ask us to restrict how they use your personal data. Your rights are set out at Article 18 of the GDPR. You can find our contact details in section 8 above.

This is not an absolute right, and your personal data may still be processed where certain grounds exist. This is:

- With your consent;
- For the establishment, exercise, or defence of legal claims;
- For the protection of the rights of another natural or legal person;
- For reasons of important public interest

Only one of these grounds needs to be demonstrated to continue data processing. We will consider and respond to requests received, including assessing the applicability of these exemptions. Please note that given the importance of ascertaining eligibility and preventing fraud, financial crime and money laundering it will usually be appropriate to continue processing personal data - in particular, to protect the rights of another natural or legal person, or because it's an important public interest of the United Kingdom.

12. Who can I complain to if I'm unhappy about the use of my personal data?

Experian tries to deliver the best customer service levels, but if you're not happy you should contact us so we can investigate your concerns.

Post: Experian, PO BOX 8000, Nottingham, NG80 7WF

Email: uk.dpo@experian.com.

If you're unhappy with how we have investigated your complaint, you have the right to refer it to the Financial Ombudsman Service (Ombudsman) for free. The Ombudsman is an independent public body that aims to resolve disputes between consumers and businesses like Experian. You can contact them by:

1. Phone on 0300 123 9 123 (or from outside the UK on +44 20 7964 1000)
2. Email on complaint.info@financial-ombudsman.org.uk
3. Writing to Financial Ombudsman Service, Exchange Tower London E14 9SR
4. Going to their website at http://www.financial-ombudsman.org.uk/

You can also refer your concerns to the Information Commissioner's Office (or ICO), the body that regulates the handling of personal data in the UK. You can contact them by:

1. Phone on 0303 123 1113
2. Writing to them at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF
3. Going to their website at http://www.ico.org.uk/

13. Where can I find out more?

The work Experian does is very complex, and this document is intended to provide only a concise overview of the key points specifically related to the ID&F business. More information about Experian and what it does with personal data is available at the following location: www.experian.co.uk/

The Information Commissioner's Office also publishes advice and information for consumers in its Credit Explained leaflet, which has references to fraud prevention and is available at

https://ico.org.uk/media/for-the-public/documents/1282/credit-explained-dp-guidance.pdf.