CONTRACT HIRE

USING MY INFORMATION

How we use your personal data

When you applied for a financial product or service with Hyundai Capital UK Limited trading as Kia Finance you will have been given a Data Protection Statement, explaining how we would treat your personal data.

This document provides you with more information about this, together with details of your personal data rights.

Contents

The Data Protection Statement explained	**2**
Fraud prevention agencies explained	**6**
Credit reference agencies explained	**7**
Your personal data rights explained	**8**
Glossary of terms	**10**

1. The Data Protection Statement explained

Data Protection Statement section	Explanation
Introduction	This section sets out who the Data Controller is and provides contact details for the Data Protection Officer. Hyundai Capital UK Limited, trading as Kia Finance and Santander Consumer (UK) Plc ("SCUK") are joint data controllers of your personal data. This means that Kia Finance and SCUK jointly decide the purposes and means of the processing of your information. References to "we", "our" and "us" in this statement are references to Kia Finance and SCUK as joint data controllers, unless the context otherwise permits. If you have any questions about how your personal data is used, or the information included in this booklet, our Data Protection Officer (DPO) can be contacted at Kia Finance, 86 Station Road, Redhill RH1 1SR
The types of personal data we collect and use	The sort of personal data we collect and use will vary depending on the products or services you require or have, and your preferred relationship with us.
Whether providing your personal data is required by law or contract or not	This section states that you'll be told whether the provision of your personal data is optional or mandatory. If the provision of the data is mandatory and we don't already hold it then you'll need to provide the information so that we can process your application or service.
Monitoring of Communications	This section explains why we may monitor your on-going communications with us. This includes us monitoring our communications with you so that we comply with regulatory rules, or our own internal processes and protocols: ▪ relevant to our business and the services we provide; ▪ to prevent or detect crime; ▪ in the interests of protecting the security of our communications systems and procedures; ▪ for quality control and staff training purposes; and ▪ when we need to access these as a record of what we have said to you/what you have said to us. For example, where we are required by Financial Conduct Authority (FCA) regulations to record certain telephone lines we will do so. Our monitoring will also check for obscene or profane content in communications. In very limited and controlled circumstances we may conduct short-term and carefully controlled monitoring of activities on your account or service. This will only be done where this is necessary for our legitimate interests, or to comply with legal obligations - for example, if we have reason to believe that a fraud or other crime is being committed, and/or where we suspect non-compliance with anti-money laundering regulations to which we are subject.
Using your personal data: the legal basis and purposes	This section describes how your personal data may be used, and the legal basis for the processing of your information. The legal basis for us processing or analysing your personal data will depend on what we're trying to achieve. Data Protection legislation allows us to process your personal data for our own legitimate interests – provided those interests don't override your own interests and/or your fundamental rights and freedoms. An example of 'legitimate interests' would be if you believed you were the victim of a fraud or scam, and you asked us to investigate your claim. To understand what has happened we may need to share your name and account number, the details of any payment(s) made and details of the case with the other bank(s) involved, so they could trace transactional activity, help to recover any of your monies that may remain and reduce the opportunity of the funds being used to support criminal activity. Therefore, the sharing of your data with the bank(s) involved falls within your legitimate interests as well as ours - to ensure that funds are prevented from being used for fraudulent and/or money laundering activities. Please note: The bank(s) we may share your data with may be located outside of the European Economic Area (EEA), and therefore may not be subject to the same data privacy legal obligations as banks within the EEA. Complying with established legal obligations is another reason for us to share your personal data. For example if you require us to transfer funds via CHAPS or internationally, your personal data may be provided to overseas authorities and the beneficiary bank to comply with applicable legal obligations and to prevent crime. This may require us to share your personal data outside of the EEA. This information may include your full name, address, date of birth and account number - and by making your payment instructions to us, you consent to us sharing personal information to overseas authorities and beneficiary bank(s) as appropriate.

Data Protection Statement section	Explanation
	Consent for processing of special categories of personal data, at your request, must be explicit. For example: ▪ If we require a copy of your passport (as a new customer) and if that reveals your racial or ethnic origin data, by providing a copy you will be explicitly consenting to us seeing your racial or ethnic origin in this way ▪ If you volunteer data concerning your health when we ask you about the conduct of your account you will be explicitly consenting to us processing this personal data in connection with your account. Under Data Protection legislation you can withdraw your consent at any time. If you do this, and if there is no alternative lawful reason that justifies our processing of your personal data for a particular purpose, this may affect what we can do for you. For example, it may mean that if you have arrears on your account, we can't take into account any personal data concerning your health, which may result in us being unable to provide you with a service that you had requested.
Sharing of your personal data	This section details when personal data may be shared, and the types of people/organisations it can be shared with. We may share your personal information with companies and other persons providing services to us. This may include data back-up and server hosting providers, our IT software and maintenance providers, and/or their agents which will use your information to better understand you as a customer and for reporting and analysis purposes to assist in the development and improvement of existing and new products and services. These companies will also use your information to send you marketing communications if you have consented to this. ▪ The Santander Group of companies as well as Kia Motors Ltd ('our Partners') which will use your information to better understand you as a customer and for reporting and analysis purposes to assist in the development and improvement of existing and new products and services. These companies will also use your information to send you marketing communications if you have consented to this. ▪ We engage Leasedrive Limited t/a Zenith ("Zenith") to process and manage contract hire applications and agreements on our behalf. Applications are submitted to us by your intermediary via Zenith's online portal. ▪ Credit reference agencies (including Experian, Call Credit, Equifax and Delphi) and fraud prevention agencies. Further information is provided in the following sections. ▪ Law enforcement agencies in order to detect, investigate and prevent crime (we or any fraud prevention agency may pass your information to law enforcement agencies). ▪ Third party debt collecting agencies engaged by us to recover monies owed to us. ▪ Any third party to whom we sell your debt. If we do this, you will be notified and that third party will become the data controller of your information. ▪ Your intermediary (or any intermediary that acquires your intermediary's business, as applicable) to assist us with administering your agreement (including conducting mid and end agreement reviews with you) and for them to send you marketing communications about their products and services if you have consented to this. ▪ If applicable and as advised in your customer agreement; the associated vehicle Manufacturer of the franchised intermediary where you purchased your vehicle. They will use your information to better understand you as a customer, for reporting and analysis purposes, and to assist in the development and improvement of existing and new products and services. The manufacturer will also use your information to send you marketing communications if you have consented to this. Please refer to your customer agreement for further information. ▪ Third parties acting on our behalf, such as back-up and server hosting providers, IT software and maintenance providers and their agents and third parties that provide income verification services, affordability checks and communication fulfilment services. ▪ Outsourced service providers required for compliance with a legal or regulatory obligation, provision of your account service or for marketing activities where your consent has been provided. ▪ Market research organisations engaged by us to undertake customer satisfaction surveys and market research. ▪ Courts in the United Kingdom or abroad as necessary to comply with a legal requirement, for the administration of justice, to protect vital interests and to protect the security or integrity of our business operations. ▪ Any third party who is restructuring, selling or acquiring some or all of our business or assets or otherwise in the event of a merger, re-organisation or similar event.

Data Protection Statement section	Explanation
International transfers	This section explains that where we transfer your personal data outside of the UK and European Economic Area (EEA) appropriate safeguards will be put in place to protect that data. Safeguards can include: (i) The Standard Data Protection Clauses (also known as EU Model Clauses), You can obtain a copy of these by contacting our Data Protection Officer (DPO). (ii) The US Privacy Shield and details are available here: privacyshield.gov/welcome or from our Data Protection Officer (DPO) (iii) Binding Corporate Rules, provided the recipients in other countries have obtained the requisite approvals. The published list of approvals is available here: https://ec.europa.eu/info/strategy/justice-and-fundamentalrights/data-protection/data-transfers-outside-eu/binding-corporate-rules_en or from our Data Protection Officer (DPO).
Identity verification and fraud prevention checks	This section explains that your personal data can be used to check your identity and for fraud prevention and anti-money laundering purposes. To find out more, refer to the 'Fraud prevention agencies explained' section of this booklet.
Credit reference checks	This section provides information on the sharing of your personal data with the credit reference agencies. To find out more, refer to the 'Credit reference agencies explained' section of this booklet.
Your marketing preferences and related searches	This section tells you how we may use your information for marketing and market research purposes. You can tell us at any time that you don't want to receive marketing or market research requests. You can provide your specific marketing preferences as part of your application. Equally you can contact us at any time to provide and/or update those preferences.
Automated decision making and processing	As part of the processing of your information, decisions may be made by automated means. Your information will be used to assess your credit risk using an automated decision-making technique called 'credit scoring'. Various factors help us to assess the risk; a score is given to each factor and a total credit score obtained, which will be assessed against a confidential pre-set pass score. In regard to fraud prevention checks, this means that we may automatically decide that you pose a fraud or money laundering risk if: ▪ our processing reveals your behaviour to be consistent with that of known fraudsters or money launderers, or is inconsistent with your previous submissions; or ▪ you appear to have deliberately hidden your true identity. We may also conduct automated processing of your information in other ways. In particular, we may use automated processing to analyse or predict (amongst others) your economic situation, personal preferences, interests or behaviour. This could mean that automated decisions are made about you using your information. For instance, we might do an analysis of certain customer demographics (such as your characteristics). We may also analyse triggers and events such as the maturity dates of your accounts and opening anniversaries. In some instances we may carry out automated processing and decision making to do behavioural scoring, including by looking at the accounts and products you already have with us and how they are being conducted, such as account activity, arrears and other indications of financial difficulties. We will do this where this information is relevant to the product that we think you might be interested in. This will help us to decide whether other products and services might be suitable and appropriate for you. All of this includes an element of automated processing. We will use the information gleaned from this activity to: (i) send direct marketing communications to you where you have consented to this; and (ii) decide which of our other products and services might be suitable and appropriate for you, including those which are offered by us, or by us in conjunction with our partners, or by the Santander Group of companies. This means that automated decisions and processing can help to determine what marketing communications you receive, when you receive them and what marketing activity is conducted by us or one of our third parties. In addition, when we provide a product or service to you, we take into account other information that we hold about you, including how you use this and other accounts you have with us or our group of companies.
Criteria used to determine retention periods	This section within the data protection statement explains the criteria we use when deciding how long personal data needs to be retained.

Data Protection Statement section	Explanation
Your rights under applicable Data Protection law	This section lists the various data protection rights that you have. Your personal data is protected under Data Protection legislation, and as a consequence you have a number of rights that you can enforce against us as your Data Controller. Please note that these rights do not apply in all circumstances. We will complete these requests within 28 days of receipt. Your rights include: ▪ The **right to be informed** - including about how we might process your personal data. This was provided to you in the data protection statement ▪ To have your personal data **corrected if it is inaccurate** and to have **incomplete personal data completed** in certain circumstances ▪ The right (in some cases) **to object to processing of your personal data** (as relevant). This right allows individuals in certain circumstances to object to processing based on legitimate interests, direct marketing (including profiling) and processing for purposes of statistics ▪ The right in some cases **to restrict processing of your personal data**, for instance where you contest it as being inaccurate (until the accuracy is verified); where you consider that the processing is unlawful and where this is the case; and where you request that our use of it is restricted; or where we no longer need the personal data ▪ The right **to have your personal data erased** in certain circumstances (also known as the 'right to be forgotten'). This right is not absolute – it applies only in particular circumstances, and where it does not apply, any request for erasure will be rejected. Circumstances when it might apply include: where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; if the processing is based on consent which you subsequently withdraw; when there is no overriding legitimate interest for continuing the processing; if the personal data is unlawfully processed; or if the personal data has to be erased to comply with a legal obligation. Requests for erasure will be refused where that is lawful and permitted under Data Protection law, for instance where the personal data has to be retained to comply with legal obligations, or to exercise or defend legal claims ▪ To **request access to the personal data** held about you and to obtain certain prescribed information about we process it. This is more commonly known as submitting a 'data subject access request'. This must be done in writing. This right will enable you to obtain confirmation that your personal data is being processed, to obtain access to it, and to obtain other supplementary information about how it is processed. In this way you can be aware of, and you can verify, the lawfulness of our processing of your personal data ▪ **To move, copy or transfer certain personal data**. Also known as 'data portability'. You can do this where we are processing your personal data based on consent or a contract and by automated means. Please note that this right is different from the right of access (see above), and that the types of data you can obtain under these two separate rights may be different. You are not able to obtain through the data portability right all of the personal data that you can obtain through the right of access • **Rights in relation to some automated decision-making about you, including profiling** (as relevant) if this has a legal or other significant effect on you as an individual. This right allows individuals, in certain circumstances, to access certain safeguards against the risk that a potentially damaging decision is taken without human intervention • To complain to the Information Commissioner's Office (ICO), the UK's independent body empowered to investigate whether we are complying with the Data Protection law. You can do this if you consider that we have infringed the legislation in any way. You can visit **ico.org.uk** for more information. If you seek to exercise any of your rights against us we'll explain whether or not that or those rights do or don't apply to you with reference to the above, and based on the precise circumstances of your request.
Data anonymisation and aggregation	This section explains that your personal data may be turned into statistical or aggregated data, data that can no longer identify you. Your personal data may be converted ('anonymised') into statistical or aggregated data in such a way as to ensure that you are not identified or identifiable from it. Aggregated data can't, by definition, be linked back to you as an individual. This data might be used to conduct research and analysis, including to prepare statistical research and reports. This data may be shared in several ways, including with the Santander Group companies, and for the same reasons as set out in the Data Protection Statement.

2. Fraud prevention agencies explained

Before we provide financial services and/or financing to you, we undertake a series of checks - not only to verify your identity, but also to prevent fraud or money laundering. These checks require us to process your personal data.

What we process and share
The personal data we process and share is what you've provided us with, details we've collected from you directly, and/or information we've received from third parties. This may include your:

- Name
- Date of birth
- Residential address and address history
- Proximity checking
- Contact details, such as email addresses and telephone numbers
- Financial information
- Employment details
- Identifiers assigned to your computer or other internet connected devices, including your Internet Protocol (IP) address
- Vehicle details

When we and/or the fraud prevention agencies process your personal data, we do so on the basis that we have a legitimate interest in verifying your identity and preventing fraud and money laundering, in order to protect our business and to comply with legal requirements. Such processing is also a contractual requirement of the services or financing you've requested.
We and/or the fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.
Fraud prevention agencies can hold your personal data for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to six years.

Automated decision making
As part of our personal data processing procedures, decisions may be made by automated means. This means we may decide that you could pose a fraud or money laundering risk if:

- our processing reveals your behaviour to be consistent with that of known fraudsters, or money launderers, or is inconsistent with your previous submissions/activity; or
- you appear to have deliberately hidden your true identity.

You have certain rights in relation to automated decision making processes. To find out more, refer to the 'Your personal data rights explained' section of this booklet.

Consequences of processing
If we (or a fraud prevention agency) determine that you pose a fraud or money laundering risk, we may refuse to provide the financial services or financing you've requested, to employ you, or we may stop providing existing services to you.

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you.

Data transfers
Whenever fraud prevention agencies transfer your personal data outside of the European Economic Area (EEA), they impose contractual obligations on the recipients of that data, in order to protect your personal data to the standard required in the EEA. They may also require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing.

For more information about the fraud prevention agencies that we use, and how they will process your personal data, please contact:

The Compliance Officer
Cifas
6th Floor, Lynton House
7-12 Tavistock Square
London
WC1H 9LT
Email: compliance@cifas.org.uk
Website: www.cifas.org.uk/privacy-notice

3. Credit reference agencies explained

When we process your application, we'll perform standard credit and identity checks on you with one or more credit reference agencies. Where we provide financial services for you we may also conduct periodic searches at the credit reference agencies to manage your account.

In doing this we'll supply your personal information to the credit reference agencies and they will give us information about you. This will include information from your credit application, information about your financial circumstances, and your financial history. The credit reference agencies will supply to us information that is in the public domain (including the electoral register), and shared credit, financial, and fraud prevention information.

We'll use this information to:

- assess your creditworthiness, and whether you can afford to manage the financial product in question;
- verify the accuracy of the data you've provided to us;
- prevent criminal activity, fraud and money laundering;
- manage your account(s);
- trace and recover debts; and
- ensure any offers provided to you are appropriate to your circumstances.

We'll continue to exchange information about you with the credit reference agencies while you have a relationship with us. We'll also inform credit reference agencies about your settled accounts. If you borrow and do not repay in full and on time, credit reference agencies will record the outstanding debt. This information may be supplied to other organisations via the credit reference agencies.

When the credit reference agencies receive a search from us, they will place a search footprint on your credit file that may be seen by other lenders.

If you are making a joint application, or tell us that you have a spouse or financial associate, we'll link your records together - so you should make sure you discuss the application with them in advance, and share this information with them before making the application. The credit reference agencies will also link your records together, and these links will remain on your and their files until such time as you or your partner successfully file for a 'disassociation' with the credit reference agencies to break that link.

For more information about the credit reference agencies that we use and how they will process your personal data please contact:

Call Credit
Callcredit Information Group
One Park Lane
Leeds
West Yorkshire
LS3 1EP
Phone: 0330 024 7574
Website: www.callcredit.co.uk/crain

Equifax
Equifax Ltd
Customer Service Centre
PO Box 10036
Leicester
LE3 4FS
Phone: 0333 321 4043 or 0800 014 2955
Website: www.equifax.co.uk/crain

Experian
Experian
PO Box 9000
Nottingham
NG80 7WF
Phone: 0344 481 0800 or 0800 013 8888
Website: www.experian.co.uk/crain

4. Your personal data rights explained

Your personal data is protected under Data Protection legislation, and as a consequence you have a number of rights that you can enforce against us as your Data Controller. We will complete these requests within 28 days of receipt.

Right to rectification
This right refers to having your personal data corrected if it's inaccurate, or to have any incomplete personal data completed.

To request a right to rectification you can contact us via the details shown below:

Marketing and market research opt-out
If you'd prefer not to receive up-to-date information on our products and services, or to be included in market research, you can indicate this by updating your marketing preferences at any time.

To opt-out of marketing and market research you can contact us via the details shown below:

Text or email opt-out
If you receive marketing emails or SMS and don't want to in future, please use the unsubscribe link within the email or text STOP to end SMS messages and we will remove you from all future campaigns.

Sharing of your personal data
If you open an account with us, your information will be kept after your account is closed. Your information may be shared across the Santander Group or associated companies, service providers or agents for administration purposes to:

- provide and run the account or service you have applied for, and develop and/or improve our products and services;
- identify and advise you by post, telephone or electronic media (including email and SMS) of products or services which our group of companies and our associated companies think may be of interest to you (for credit products this may involve releasing your details to a credit reference agency);
  and
- release your name, address and telephone number to market research organisations for the purpose of confidential market research surveys, carried out by post or telephone, on our behalf.

Complaints
We always strive to provide you with the best products and services. Unfortunately things can sometimes go wrong, but telling us about errors or oversights will give us the chance to fix things for you and make long-term improvements to our services.

The easiest and quickest way to get in touch about a complaint is by talking to our dedicated Complaints Team.

To talk to our dedicated Complaints Team you can contact us via the details shown below:

You may also be able to refer your complaint to the Financial Ombudsman Service. The Financial Ombudsman Service acts as an independent and impartial organisation which helps settle disputes between consumers and financial services businesses. You can find out more information at **financial-ombudsman.org.uk**.

Alternatively, you may also be able to refer your complain to the Information Commissioner's Office (ICO), the UK's independent body empowered to investigate whether we are complying with the Data Protection law. You can do this if you consider that we have infringed the legislation in any way. You can visit **ico.org.uk** for more information.

Data subject access requests
You have the right to find out what information, if any, is held about you. This is known as a data subject access request.

A data subject access request is not designed to deal with general queries that you may have about your account. We therefore aim to provide you with the information you require without you having to make a formal request. If you would like to find out specific information about your account, you can contact us by phone.

We will complete data subject access request within 28 days of receipt

To make a formal data subject access request you can contact us via the details shown below:

Data portability requests
You have the right to move, copy or transfer certain personal data. Also known as 'data portability'. This gives you the right to have certain parts of the data we hold on you transferred to you or another third party.

At Kia Finance, we will provide you with the information in a machine readable format for you to pass onto whoever you would like. We will make this available to you within 28 days of receiving your request.

To make a formal data portability request you can contact us via the details shown below:

Right to be forgotten requests

The right to have your personal data erased in certain circumstances (also known as the 'right to be forgotten'). This right means that under certain circumstances you can ask us to remove all the data we hold on you. If we are unable to fulfil this right we will let you know and the reason why. Where we can carry out this right for you we will do this within 28 days of receiving your request.

To request a right to be forgotten you can contact us via the details shown below:

Contact Details

	By Phone Kia Finance Contract Hire Call us on **0800 074 9755** Our lines are open 8:00am to 6:30pm Monday to Friday
	By Post Write to us at the address below, providing: ▪ A daytime phone number in case we need to contact you to discuss your request ▪ Your agreement number(s) ▪ Whether your request relates to a specific part of the company, for example a branch or Head Office department ▪ If your request doesn't relate to an account, please let us know the nature of your relationship with Kia Finance and any other relevant information **Kia Finance Contract Hire** One Central Boulevard Blythe Valley Park Solihull West Midlands B90 8BG

Automated decision making and processing

In some instances we'll undertake automated processing and decision-making to decide which of our other products or services might be of interest to you. You have a right not to have a decision made based solely on automated processing (including profiling) that produces legal or similar effects. This doesn't apply where the processing is necessary for the performance of a contract, is authorised by law, or the person has given their consent to the processing (though they can revoke their consent thereafter).

Where you have been adversely affected by an automated decision, and/or you think we have made a mistake, or you have further information to support your case, there is an underwriting process in place. We can't guarantee to reverse a decision, but we'll always be happy to reconsider your application if you believe you have been wrongly declined.

To ask us to reconsider your application you can contact us:

	By Post Write to us at the address below, providing your name, address and proposal number. **Underwriting Review Unit** Kia Finance 86 Station Road Redhill RH1 1SR

Glossary of terms

Behavioural scoring
Techniques that help organisations decide whether or not to grant credit to customers.

Beneficiary bank
A beneficiary bank is the receiving bank where you have your account.

Binding Corporate Rules
Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or a group of enterprises engaged in a joint economic activity.

Biometric data
Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or things like fingerprints.

CHAPS
Clearing House Automated Payment System.

Data Controller
The natural or legal person, public authority, agency or other body which along or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. Data Protection Officer A person charged with advising the controller or processor on compliance with data protection legislation and assisting them to monitor such compliance.

Disassociation
A disassociation is a method of removing a financial connection between individuals that have been connected together as financial associates at the credit reference agencies. When people have joint accounts or they live together where their earning and spending behaviour affects each other, information on these financial relationships is taken into account when individuals apply for credit. Credit reference agencies hold this information as 'financial associations'. If an individual has been incorrectly linked to someone else or all financial ties have been broken so there are no longer any shared finances such as income or spending, then an individual can request for a 'disassociation' at the credit reference agencies.

EEA
The European Economic Area (EEA) is the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, including the freedom to choose residence in any country within this area. The EEA includes the EU countries as well as Iceland, Liechtenstein and Norway.

Legal basis
The legal basis for processing personal data.

Legitimate interest
The lawful grounds for data processing. Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Personal data
'Personal data' means any information relating to an identified or identifiable natural person ('Data Subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Processing
Processing means any operation or set of operations which is performed on personal data or on sets of personal data, where or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special categories of personal data
The special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data or data concerning an individual's sex life or sexual orientation, and the processing of genetic data or biometric data for the purpose of uniquely identifying an individual.

US Privacy Shield
The framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States, providing companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the EU and Switzerland to the United States.