



In this Privacy Notice according to Art. 13, 14 GDPR we are informing you about the automated, electronic processing of your personal data by AUDI AG, Auto-Union-Straße 1, 85057 Ingolstadt, Deutschland / Germany (“**we**”, or “**Audi**”) as a business partner or employee of a business partner.

Personal data means any information relating to an identified or identifiable natural or, if foreseen under local law, legal person, including, as the case may be, sensitive personal data as defined under the laws of the country where you are located at the relevant time (‘data subject’); a data subject is one that can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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

1. Who is the controller for the processing?

The **controller** for the processing of your personal data is:

AUDI AG, Auto-Union-Straße 1, 85057 Ingolstadt, Germany.

Tax identification number/Registration number: DE811115368; HRB Nr./Commercial Register No.: HR B 1

2. Who can I contact?

If you wish to assert your data protection rights, please use the contact options at

<https://data-subject-rights.audi.com/>

There, you will find further information regarding how you can assert your data protection rights. You may also send your request

- via mail: AUDI AG, DSGVO-Betroffenenrechte, 85045 Ingolstadt, Germany

We take data subject rights very seriously and will respond to any request that you might have as soon as possible. If you have any general questions about this privacy notice or the processing of your personal data by AUDI, please use the following contact option:

e-mail: dsgvo-beschaffung@audi.de

3. Contact details of the data protection officer

For matters concerning data protection, you can also consult our **company data protection officer**, using your own language:

AUDI AG, Data Protection Officer, 85045 Ingolstadt, Germany

- Email: datenschutz@audi.de
- Telephone number: +49841 890
- Office address of the company data protection officer: AUDI AG, Data Protection Officer, Auto-Union-Straße 1, 85057 Ingolstadt, Germany

4. Which rights do I have?

All the below described rights concerning the personal data and the processing thereof may be subject to limitations, according to the applicable EU and / or national laws. Depending on your jurisdiction, as the data subject, you may be



entitled to the following data protection rights. **Please note:** Your data protection rights under the local laws of the country where you are located at the relevant time may differ from the rights described below.

As a data subject, you are generally entitled to the following data protection rights:

Access: You have the right to request information about the data stored about you at Audi and the scope of the data processing and disclosure carried out by Audi and to receive a copy of the personal data stored about you.

Rectification: You have the right to obtain without undue delay the rectification of inaccurate personal data concerning you as well as the completion of incomplete personal data stored concerning you at Audi.

Erasure: You have the right to obtain the erasure of the personal data concerning you stored at Audi without undue delay if the statutory requirements are met.

This may be the case, in particular, if

- Your personal data are no longer necessary in relation to the purposes for which they were collected;
- The sole legal ground for the processing was your consent and you have withdrawn it;
- You have objected to the processing based on the legal ground of legitimate interests on grounds relating to your particular situation and we cannot prove that there are overriding legitimate grounds for the processing;
- Your personal data have been unlawfully processed; or
- Your personal data have to be erased for compliance with a legal obligation.

If we have shared your data with third parties, we will inform them about the erasure, insofar as required by law.

Please note that your right to erasure is subject to restrictions. For example, we are not required or allowed to delete data that we are still obligated to retain due to statutory retention periods. Similarly, data that we need for the establishment, exercise or defence of legal claims are excluded from your right of erasure.

Restriction of processing: You have the right to obtain, under certain conditions, restriction of processing (i.e. the marking of stored personal data in order to restrict their future processing). The requirements are, in particular:

- The accuracy of your personal data is contested by you and Audi must verify the accuracy of your personal data;
- The processing is unlawful, but you oppose the erasure of the personal data and instead request the restriction of the use of the personal data;
- Audi no longer needs your personal data for the purposes of processing, but you require the data for the establishment, exercise or defence of legal claims;
- You have objected to the processing and the verification is pending whether the legitimate grounds of Audi override yours.

In the event of a restriction of the processing, the data will be marked accordingly and will be – except for their storage – only processed with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or of a EU Member State or of the country where you are located at the relevant time, in each case only to the extent permitted under applicable data protection laws.

Please note that the restriction of the processing of your personal data may be also employed as an alternative to the erasure of your personal data, where permitted by applicable law.



Data portability:	To the extent that we automatically process your personal data provided to us based on your consent or a contract with you (including your employment contract), you have the right to receive the data in a structured, commonly used and machine-readable format and to transfer those data to another controller without hindrance from Audi. You also have the right to have the personal data transferred directly from Audi to another controller where technically feasible and provided that this does not adversely affect the rights and freedoms of others.
Objection:	If we process your personal data on the basis of legitimate interests or in the public interest, you have the right to object to the processing of your data on personal grounds. In addition, you have an unrestricted right to object if we process your data for our direct marketing. Please see our separate note in the "Information on your right to object" section.
Withdrawal of consent:	If you have given consent to the processing of your personal data, you may withdraw it at any time. Please note that the withdrawal shall only be effective for the future. Processing that occurred before the withdrawal shall not be affected.
Complaint:	In addition, you have the right to lodge a complaint with a data protection supervisory authority if you believe that the processing of your personal data is unlawful. The right to lodge a complaint is without prejudice to any other administrative or judicial remedy. The address of the data protection supervisory authority responsible for Audi is: Bayerisches Landesamt für Datenschutzaufsicht Promenade 18 91522 Ansbach Deutschland / Germany

However, you can also lodge a complaint with any other data protection supervisory authority competent for you within or outside the EU, in particular with the one in the Member state of your habitual residence, place of work or place of the alleged infringement. Please find hereinafter a link where you can find all contact details of the national authorities in all member states:

https://edpb.europa.eu/about-edpb/board/members_en

In case you are resident in Japan, you also have the right to lodge a complaint with the Japanese authority, PPC as below:

Personal Information Protection Commission, Government of Japan (PPC), Kasumigaseki Common Gate West Tower 32nd Floor, 3-2-1, Kasumigaseki, Chiyoda-ku, Tokyo, 100-0013, Japan

Telephone number: [+81-3-6457-9680](tel:+81-3-6457-9680)

See Appendix 1 "Additional rights of data subjects and further country-specific information" for contact details of national supervisory authorities and further country-specific information.



Information on your right to object

Right to object on grounds relating to your particular situation

You have the right to object to the processing of your personal data on grounds relating to your particular situation. The prerequisite for this is that the data processing takes place in the public interest or on the basis of legitimate interests. This also applies for any profiling.

Insofar as we base the processing of your personal data on legitimate interests, we generally assume that we can demonstrate compelling legitimate grounds, but we will, of course, examine each individual case.

In the event of an objection, we will no longer process your personal data, unless,

- we can demonstrate compelling legitimate grounds for the processing of such data which override your interests, rights and freedoms or
- your personal data are used for the establishment, exercise or defence of legal claims.

Objection to the processing of your data for our direct marketing purposes

Where we process your personal data for direct marketing purposes, you have the right to object at any time to the processing of personal data concerning you for such marketing; this also applies to profiling to the extent that it is related to such direct marketing. If you object to the processing for direct marketing purposes, we will no longer process your personal data for such purposes, which includes profiling to the extent that it is related to such direct marketing.

If you object to processing for direct marketing purposes, we will no longer process your personal data for these purposes.

Objection to the processing of your data for product improvement and general customer analysis

As part of the legitimate interests, we grant you a separate right of objection with regard to the processing of your personal data for product improvement and general customer analysis.

If you object to the processing for the purpose of product improvement and/or general customer analysis, we will no longer process your personal data for these purposes. Purely statistical evaluations of aggregated or otherwise anonymous data remain unaffected by this.

Exercise of the right to object

The objection can be exercised in any form and should preferably be addressed to the contact details listed in this privacy notice.



5. Which data do we process?

We process personal data which we receive from you within the scope of our business relationship with you as a business partner or employee of a business partner.

The personal data include:

- Private contact and master data
 - Contact details (private)
 - Credentials
- Professional work and organizational data
 - Contact details (professional)
 - Work organization assignment(s)
- IT usage data
 - User and login data
 - Logging data (security-relevant)
 - Logging data (operational safety-relevant)
 - Logging data (subject-related)
 - Software and hardware data
- Recordings
 - Shots
 - Photographs
 - Recordings
- Vehicle master data and identification
 - Vehicle identification data
 - Vehicle master data
- Vehicle usage data (vehicle usage and operating data)
- Location
 - Stationary location data
 - Location history data
- Legal Transactions / Contract Data
 - Contract metadata
 - Power of attorney and representation
- Financial data
 - Creditworthiness data (incl. score values)
 - Assets and ownership
 - Payment data and bank information
- Particularly sensitive personal data
 - Health
 - Biometric data
- Data on criminal offences / administrative offences

As part of internal investigations, e.g. in connection with whistleblower reports or the investigation of data protection breaches, we may process additional data where applicable.

6. For which purposes do we process your data and which legal bases apply?

We process your personal data in accordance with the provisions of the General Data Protection Regulation ("GDPR") and the German Federal Data Protection Act (Bundesdatenschutzgesetz, "BDSG") and other applicable local laws for various purposes.



The processing of your personal data must be based on one of the following legal bases:

- You have given your consent (Art. 6(1)(a) GDPR);
- Processing is necessary for the performance of a contract with you or in order to take steps at your request prior to entering into a contract (Art. 6(1)(b) GDPR);
- Processing is necessary for compliance with a legal obligation under EU law or the law of an EU member state to which we are subject (Art. 6(1)(c) GDPR);
- Processing is necessary in order to protect your vital interests or those of another person (Art. 6(1)(d) GDPR);
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us (Art. 6(1)(e) GDPR)
- Processing is necessary for the purposes of the legitimate interests pursued by Audi or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data, in particular where the data subject is a child (Article 6(1)(f) GDPR).

If, in exceptional cases, we process special categories of personal data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sex life or sexual orientation) about you, one of the following legal bases must also apply:

- You have given your explicit consent (Art. 9(2)(a) GDPR);
- The processing is necessary to protect your vital interests or those of another person and the data subject is physically or legally incapable of giving consent (Art. 9(2)(c) GDPR);
- the processing relates to personal data which you have manifestly made public (Art. 9(2)(e) GDPR)
- processing is necessary for the establishment, exercise or defence of legal claims (Art. 9(2)(f) GDPR)
- processing is necessary for reasons of substantial public interest on the basis of EU law or the law of an EU Member State which is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard your fundamental rights and interests (Art. 9(2)(g) GDPR).

Following on from the above, we process your personal data on the basis of the following legal bases for the following purposes

Purpose	Examples of data processing	Legal grounds	Legitimate basis	Categories of data
Claims management		Fulfilment of contracts, balancing of interests	Communication with tortfeasors or injured parties, efficient handling of claims by or at AUDI	
Contract management (other contracts), in particular business partner management		Legitimate interests, fulfilment of contract, consent	Fulfilment of legal requirements of AUDI dealers, professionalisation of the AUDI brand image and improvement of the experience for customers through qualification of the employees of our trade and business partners; improvement of cooperation with trade and business partners	Professional work and organisational data; IT usage data



Customer enquiries and customer complaints		Contract fulfilment (e.g. service contract, vehicle purchase contract or contract for special equipment) and consent, legitimate interests	Control of product quality and prevention of product damage, preventive complaint management	Professional work and organisational data; IT usage data; Recordings
Customer order processing, including vehicle production and provision of digital services	Provision of products, services and services within the framework of and in advance of contractual relationships; Registration and customer accounts; Event and complaint analysis	Performance of the contract (e.g. service contract, vehicle purchase contract or contract for special equipment), consent		
Development and testing of components, products and services	Development, testing of new products and improvement and optimisation of existing products, services and offers; Participation in research collaborations; Provision of products, services and services within the framework of and in advance of contractual relationships	Fulfilment of the contract (e.g. service contract, vehicle purchase contract or contract for special equipment) and consent, balancing of interests	Improvement of road safety and own products, promotion of science	
Event and participant management	Event	Balancing of interests, consent if necessary	Preparation and follow-up and implementation of events, improvement of the organization for the future	
Internal administration		Performance of contract, balancing of interests, fulfilment of legal obligations, consent if necessary	Analysis of sales and order data by model, sales channel, order status; - Analysis of demanded variants and equipment; Reporting on business parameters, if necessary using the VIN; Execution of evaluations to control our business processes and cost control on the basis of the analysis of sales and	



			order data according to the model, sales channel, order status, analysis of requested variants and equipment, reporting on business parameters, if necessary using the vehicle identification number; Maintenance of operations; Compliance with legal and regulatory requirements; Granting benefits and support to employees; Maintaining product quality; Prevention of recourse claims; Preparation and follow-up of events, improvement of the organization for the future,	
IT security		Legitimate interests	Protection of the IT infrastructure against accidental or wilful damage, recovery of data after data loss to maintain the IT infrastructure	Professional work and organisational data; IT usage data
Knowledge management and contact management		Balancing of interests	Acquisition, development, transfer, storage and use of knowledge in the organization	
Legal affairs and compliance		Compliance with a legal obligation, public interest, fulfilment of legal obligations, legitimate interests, fulfilment of contract	Compliance with legal and regulatory requirements; Verification of compliance with legal provisions, internal company guidelines, rules and standards of Audi, Group companies, employees, business partners and other third parties; Compliance with legal and regulatory requirements, assertion, exercise or defence of legal claims of Audi or the respective AUDI dealer; Verification of compliance with contractual and legal obligations by Audi, its employees and its sales partners, suppliers, etc., if necessary using the vehicle identification number	Professional work and organisational data; IT usage data; Recordings; Legal transactions / contract data; Particularly sensitive personal data
Logistics and passenger transport as well as fleet management		Fulfilment of contracts, balancing of interests	Organization and maintenance of the vehicle fleet	Representation of AUDI AG and representation of its interests
Operation and administration of and/or support for internally used IT systems		Legitimate interests	Protection of the IT infrastructure against accidental or wilful interference, maintenance of IT systems and security	Professional work and organisational data; IT usage data
Operational safety and emergency management, owner's or tenant's right to		Fulfilment of legal obligations, legitimate interests, consent	Maintaining plant safety, access control, accident prevention	Professional work and organisational data; IT usage data; Recordings



undisturbed possession of premises and to keep out trespassers				
Order placement, external and internal projects, including construction management		Legitimate interests	Maintaining operations and improving production	Professional work and organisational data; IT usage data; Legal transactions / contract data
Prevention of violations of the law (especially criminal offences) and abuse	Compliance checks, fraud and money laundering prevention	Fulfilment of legal obligations, balancing of interests	Compliance with legal and regulatory requirements; Verification of compliance with legal provisions, internal company guidelines, rules and standards of AUDI AG, group companies, employees, business partners and other third parties	
Public relations, lobbying and communication with authorities	Public relations, lobbying and communication with associations and authorities; Statutory reporting obligations	Fulfilment of a legal obligation, balancing of interests		
Review and optimization of systems, procedures and processes	Product development, testing, testing and quality assurance; Product monitoring; Callbacks	Balancing of interests	Control of product quality and prevention of product damage, preventive complaint management	
Supplier management including supplier analysis and evaluation		Legitimate interests	Systematic management of relationships with suppliers, identification and evaluation of potential suppliers, supplier coaching and improvement of supplier relationships.	Professional work and organisational data; IT usage data; Legal transactions / contract data

Please note: If the applicable local law of the country where you are located at the relevant time foresees additional requirements regarding the legal bases, we will comply with such additional requirements and will inform you accordingly. This in particular applies, where such local law requires (express) consent for the processing of your personal data.

Please note your rights to object to the processing of data for the purpose of direct marketing or for personal reasons and your right to withdraw consent (see Sec. 4 "Which rights do you have?" and the "Information on your right to object").

7. Is there an obligation to provide personal data?

As part of our business relationship or interaction, you only need to provide the personal data that is required for the interaction, or that we are required to collect by law. Without this data, we will generally have to refuse to enter into the contract or to execute the order, or will be unable to perform an existing contract and possibly have to terminate it.



If we are asking you for your consent to the processing of your personal data, such consent will always be voluntary. However, if you do not give your consent, we might not be able to provide a particular service, if the relevant service cannot be provided without such data.

8. Who receives my data?

8.1. Data processing under the joint responsibility of Audi and Volkswagen Group Companies

We also process such personal data of yours that is stored in the ONE.Konzern Group Business Platform of the Volkswagen AG. Personal data processed in conjunction with the ONE.Konzern Group Business Platform is subject to joint responsibility by Audi and affiliated Volkswagen Group companies (hereinafter referred to as "**Volkswagen Group Companies**"). Consequently, these entities may have access to your personal data. For more information on the processing of your personal data in connection with the ONE.Konzern Group Business Platform and related data processing within the framework of joint responsibility between Audi and the Volkswagen Group Companies please refer to the following links. The links also provide you with information about the Volkswagen Group Companies and third-party providers involved in the provision of the ONE.Konzern Group Business Platform, including potential third country transfers as mentioned under Sec. 9 below:

ONE.Konzern Business Plattform (Startseite): <http://www.vwgroupsupply.com>

- Data Protection Information of ONE.Konzern Business Plattform
https://www.vwgroupsupply.com/one-kbp-pub/de/kbp_public/rechtliches_4/privacy_policy/privacy_policy_1.html
- Data Protection Information of the Volkswagen Group Brands and Companies
[Datenschutzerklärungen von Konzernunternehmen](#)
- List of enclosed Volkswagen Group Companies
https://www.vwgroupsupply.com/one-kbp-pub/media/kbp_public/documents_2/rechtliches_3/liste_der_konzerngesellschaften_1/Liste_der_Konzerngesellschaften.pdf

8.2. Data processing under the sole responsibility of Audi

Within Audi, those teams receive your data that need it in connection with their work (e.g. Technical Development, IT).

Service providers which are used and act on behalf of us and that do not process data for any of their own purposes (so called "processors") may receive data for the purposes mentioned above. We utilise processors of the following categories for the provision of specific services, who support us in the execution of our business processes. Specifically, this includes entities affiliated with us (hereinafter referred to as "**Group Companies**").

These processors include:

- Service providers/suppliers
- Creditors and opposing parties in legal disputes
- Business partners
- Group companies

In addition, data may be shared with public authorities, and public corporations, and interest groups, including security authorities, to the extent we should be required to do so by law or by enforceable regulatory or judicial orders. We will generally share your personal data with third parties only if this is necessary for the performance of the contract, if we or the third party have a legitimate interest in the disclosure, or if you have given your consent, subject to applicable local laws. Third parties to whom we disclose your personal data for the purposes mentioned above and who act as data controllers under data protection law include

- Authorities
- Service providers/suppliers



- Insurance companies
- Creditors and opposing parties in legal disputes
- Healthcare institutions / physicians
- Business partners
- Group companies
- Public-law bodies and interest groups
- Legal, business, and financial representatives
- Media companies / press
- Legal, business, and financial representatives
- Subsidiaries
- Insurance companies

9. Is data transferred to a third country?

We process your data in Germany. As a rule, we do not transfer your data to other countries or third countries (countries that are neither members of the European Union nor the European Economic Area) or to international organisations.

A transfer of data to third countries (i.e. countries that are neither members of the European Union nor of the European Economic Area) may take place, to the extent this is required for the provision of services to you, is required by law, or you have given us your consent (in the absence of any other appropriate safeguarding mechanism under applicable law).

Please note: Under the applicable local laws of the jurisdiction where you are located at, a transfer to a third country might be defined as a transfer outside of the territory or country where you are located at the relevant time.

Please note that not all third countries have a level of data protection recognised as adequate by the competent body of the country where you are located at the relevant time (e.g. the European Commission). Audi will only transfer your personal data to third countries to the extent permitted by applicable law. Insofar as Audi relies on appropriate safeguards in accordance with applicable law (e.g. Standard Contractual Clauses or Binding Corporate Rules pursuant to Art. 46(2) GDPR for third country transfers), Audi will take such additional technical and/or organizational measures to the extent necessary to maintain an adequate level of protection of your personal data, as required under applicable laws.

With regard to use of the ONE.Konzern Business Platform and in connection with groupwide processes, we also transmit your data to Volkswagen AG Group Companies outside the European Union or the European Economic Area. You will receive information about the companies that receive access to your data on the ONE.Konzern Business Platform, on the platform. Our contract-based processors in certain cases also process personal data in countries outside the European Union or the European Economic Area.

Exceptions may also arise if you are employed by a business partner with headquarters in a third country or an event takes place in third countries. In addition, some of our IT service providers or other business partners, customers, or suppliers may be located in third countries. In certain cases, personal data may also be shared with officials and courts in third countries.

You can obtain a copy from us of the specific applicable or agreed rules to ensure the adequate level of data protection. Please use the information in the Contact section for this purpose.

Your data will be transferred to the following recipients in a third country: Volkswagen Group Companies, who may request services from you. List of enclosed Volkswagen Group Companies:

https://www.vwgroupsupply.com/one-kbp-pub/media/kbp_public/documents_2/rechtliches_3/liste_der_konzerngesellschaften_1/Liste_der_Konzerngesellschaften.pdf.



10. How long will my data be stored?

We store your data as long as it is necessary for the purpose for which we have collected the data or we have a legitimate interest in the further storage. In other words, we routinely process and store your personal data for the duration of our business relationship with you or the business partner for which you work or your interaction with us.

In addition, we are subject to various retention and documentation obligations, which result, inter alia, from the German Commercial Code (*Handelsgesetzbuch*, "HGB") and the German Tax Code (*Abgabenordnung*, "AO"). The periods specified therein for retention and documentation are up to ten years. Finally, the storage period is also assessed according to the statutory limitation periods, which can be up to thirty years, for example, according to Sections 195 et seqq. of the German Civil Code (*Bürgerliches Gesetzbuch*, "BGB"), with the regular period of limitation being three years.

Under certain circumstances, your data may also need to be retained for a longer period of time, such as when a so-called *legal hold* or *litigation hold* (i.e. a prohibition of data deletion for the duration of the proceedings) is ordered in connection with administrative or judicial proceedings.

We may also be subject to retention and documentation obligations in line with the local legislation of your country.

11. What practices and procedures are implemented to secure my data?

We have implemented and maintain at all times encompassing technical and organisational measures (*TOMs*) to protect your data in accordance with the high standards of the GDPR and the standards required under other applicable local laws of the jurisdiction you may be located at. This includes, but is not limited to, pseudonymisation and encryption, measures to ensure the ongoing confidentiality, integrity and availability of your data (including the ability to restore data in case of an incident). We are regularly reviewing our TOMs and apply enhancements where needed to keep your data safe and to comply with applicable laws. We have put in place appropriate procedures to deal with any personal data breach (i.e. a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed) and will notify you as the data subject and relevant supervisory authority when we are legally required to do so.

12. Updates of this privacy notice

We might update this privacy notice from time to time by making available updates to this privacy notice on our website.

Anex 1: Additional data subject rights and further country-specific information



Argentina

We process your personal data on the basis of the following legal bases for the following purposes:

Please refer to the table in Sec. 6.

Purpose	Legal grounds	Categories of data
Implementation of employment, HR administration and employer duties (communication & management, work organisation, HR service)	Fulfilment of contract, consent, compliance with a legal obligation	Professional work and organisational data
Supplier management including supplier analysis and evaluation	Consent	Professional work and organisational data; IT usage data; Legal transactions / contract data
Order placement, external and internal projects, including construction management	Consent	Professional work and organisational data; IT usage data; Legal transactions / contract data
Contract management (other contracts), in particular business partner management	Fulfilment of contract, consent	Professional work and organisational data; IT usage data
IT security	Consent	Professional work and organisational data; IT usage data
Operation and administration of and/or support for internally used IT systems	Consent	Professional work and organisational data; IT usage data
Operational safety and emergency management, owner's or tenant's right to undisturbed possession of premises and to keep out trespassers	Fulfilment of legal obligations, consent	Professional work and organisational data; IT usage data; Recordings
Legal affairs and compliance	Compliance with a legal obligation, public interest, fulfilment of legal obligations, consent, fulfilment of contract	Professional work and organisational data; IT usage data; Recordings; Legal transactions / contract data; Particularly sensitive personal data
Customer enquiries and customer complaints	Contract fulfilment (e.g. service contract, vehicle purchase contract or contract for special equipment) and consent	Professional work and organisational data; IT usage data; Recordings



You have the right to

- access;
- rectification;
- erasure;
- file a complaint regarding the processing of your personal data to THE PUBLIC INFORMATION ACCESS AGENCY, which, depending on the facts of the individual case, in its capacity as the Control Entity of Law No. 25,326, has the power to attend complaints and claims filed by those whose rights are affected due to breaches with applicable regulations on personal data protection.

Australia

You have the right to

- access;
- rectification;
- lodge a complaint with both Audi and the Office of the Australian Information Commissioner (“OAIC”) or any other dispute recognition scheme recognised by the OAIC which can be found on the OAIC website www.oaic.gov.au.

If you are concerned with the way we have handled your personal data, you may lodge a privacy complaint with the Office of the Australian Information Commissioner (“OAIC”). However, it is a requirement of the OAIC that prior to lodging a complaint, you have raised your complaint with us. If you are not satisfied with our response or we fail to provide a response within 30 days of receipt, you can lodge a complaint with the OAIC. The contact details for the OAIC are set out below:

Phone	1300 363 992
Fax	(02) 9284 9666
Website	https://www.oaic.gov.au/
Post	GPO Box 5288, Sydney NSW 2001

Brazil

You have the right to

- to be informed about the collection and use of your personal data, by us, in a readily accessible manner, and in plain and clear language. You also have the right to be informed about any public or private entity with whom your data has eventually been shared. We are implementing your right to be informed, also through this notice, the content of which may be updated from time to time.
- information access;
- obtain a copy when the legal basis for processing is consent or performance of a contract;
- erasure when consent is the legal basis for processing: please note that exceptions to this right might apply, namely, when the data is needed for (i) compliance with legal obligations; (ii) study by a research organization; (iii) transfer to third parties; (iv) use solely by the controller, as long as the data is anonymized;
- rectification;
- object to the processing (e.g. if the data is being unlawfully processed);



- data portability;
- withdraw consent at any time;
- anonymize, block or delete unnecessary or excessive personal data or data processed in noncompliance with data protection law;
- review decisions made solely on the basis of automated processing;
- lodge a complaint before ANPD (Autoridade Nacional de Proteção de Dados) against the data controller;
- be informed of the possibility of not providing consent and the consequences thereof;
- be informed about the public and private entities with whom the data has been shared.

Canada

Please note

Personal data may be processed or stored outside of Canada for purposes consistent with this Data Protection Notice. You acknowledge and agree that, as a result, the personal data that is processed or stored or accessed in other jurisdictions may be subject to the laws of those jurisdictions and may be disclosed in response to valid demands or requests from government authorities, courts, or law enforcement in such other countries.

Under Canadian law, you have the right to

- opt out of information handling practices that are not reasonably necessary to provide the services you've requested. You can exercise this right by contacting using the contact details set out in Sec. 2.
- be informed of the use by us of technology allowing us to profile, locate or identify you and of the means available to you to activate the functions that allow us to identify, locate or profile you.

While Audi takes the security of personal data seriously and uses industry standard security risks associated with transferring and processing personal data contemplated herein. However, no security or processes are fool proof. If personal data is accessed by third parties, it may lead to phishing attempts to get more information from you and/or identify theft.

China

The following supplements and/or amendments to the privacy notice apply if you are located in the People's Republic of China (excluding Hong Kong Special Administrative Region, Macao Special Administrative Region, Taiwan) pursuant to the local data protection laws in China, which include the PRC Personal Information Protection Law. In the event of any conflict or inconsistency between the privacy notice the following shall govern and prevail:

Collection and Use of Personal Data

Specifying the information provided in Section 1 we may process the following sensitive data:

n/a

In cases where sensitive personal data is actually collected, we will use enhanced notification or instant alerts (e.g., pop-up reminders) to remind you and obtain your authorization again, or require you to click on a separate confirmation, or sign a separate consent letter.

Legal Basis for Processing Personal Data

We only process your data if and to the extent we can rely on a legal basis for such processing under the laws of China, i.e.

- (i) where the consent of the individual concerned is obtained;



(ii) where it is necessary for the conclusion or performance of a contract to which the individual concerned is a party, or for the implementation of human resources management in accordance with the labor rules and regulations formulated in accordance with the law and the collective contract concluded in accordance with the law;

(iii) where it is necessary for the performance of statutory duties or statutory obligations;

(iv) where it is necessary for the response to a public health emergency or for the protection of the life, health and property safety of a natural person in an emergency;

(v) where such acts as news reporting and supervision by public opinions are carried out for the public interest, and the handling of personal data is within a reasonable scope;

(vi) where it is necessary to handle the personal data disclosed by the individual concerned or other personal data that has been legally disclosed within a reasonable scope in accordance with the provisions of the Law; and

(vii) other circumstances prescribed by laws and administrative regulations.

Personal Data We Share

For the purposes stated in the privacy notice, we may share your personal data with

- service providers. We will make agreement on strict data protection measures with our service providers and request our service providers to process the related data in accordance with our designated purposes, service descriptions, this privacy notice and any other related confidentiality and security measures.
- third parties who have their own purposes and means of processing your personal data as provided in below. We will not disclose you personal data to public or to third parties, except we obtain your separate consent.

Relevant third parties are listed in Section 8. We should obtain your separate consent before sharing your personal data to the aforementioned third parties. If the recipient changes the original purpose or method of treatment prescribed in this privacy notice, he or she shall obtain the consent of the individual again in accordance with the provisions of the Law.

Transfer of data to countries outside of China

Generally, we store personal data collected and generated from China in our data center and on cloud servers in EU/EEA area that we rent (or commission third-party service providers to rent). As we offer products or services through resources and servers around the world, which means with your separate consent, your personal information may be transferred to Germany or others third countries. Please refer to Section 9 for further information.

We will conduct an impact assessment of personal data protection in accordance with local laws in China, and complete the security assessment organized by the national network information department and/or the personal information protection certification by professional institutions in accordance with the provisions of the national network information department and/or execute the standard contract formulated by the national network information department with the recipient, stipulating the rights and obligations of our overseas recipients. If you need to exercise your right to protect your personal information to the overseas recipient, you can contact us using the contact details set out in Sec. 2. We will help you, in general, within 30 working days, unless otherwise provided by laws and regulations.

Your Rights

Except all the subject rights indicated under Section 4 of this privacy notice, you may:

- request that we transfer certain personal data we hold about you to your designated entities when you meet the conditions specified by applicable Chinese laws.
- request us to erase your personal data when:
 - The processing purpose has been achieved or cannot be achieved, or your personal data is no longer necessary to achieve the processing purpose;
 - We cease the provision of products or services for which your personal data is being processed, or the retention period has expired;
 - You withdraw consent to the processing (if the processing is based on your consent);
 - We process personal data in violation of law or any agreements with you; or



- Your personal data must be deleted in accordance with applicable Chinese laws.
- lodge a complaint.

If you have any questions, comments or suggestions about this Notice or matters related to your personal data or you intend to exercise your rights, please use the contact options at <https://data-subject-rights.audi.com/> or send your request via mail: AUDI AG, DSGVO-Betroffenenrechte, 85045 Ingolstadt, Germany. Audi will usually reply within 15 working days, unless otherwise provided by laws and regulations. We may not be able to respond to your request if your request is related to the performance of our obligations under laws and regulations, or it directly involves national security, national defense security, public health, crime investigation and other matters directly related to the public interest, or if it may lead to serious damage to the legitimate rights and interests of you or other individuals or organizations, or it is related to trade secrets.

If you are not satisfied with our reply, especially if you believe our personal data processing has harmed your legitimate rights and interests, you may also lodge a complaint with or report to the cyberspace, telecommunications, public security, industry and commerce and other regulatory authorities, or take proceedings in the court of competent jurisdiction.

How we store and protect your personal data

- We promise that, unless otherwise required by laws and regulations, we will store your personal data for the shortest period of time necessary to achieve the purposes for which you have authorized the use of your personal data, unless otherwise provided by laws and regulations or regulatory documents. After the above-mentioned period of storage of personal data, we will delete or anonymize your personal data.
- We use reasonably practicable security measures (e.g. security control, access and download rights control, improper access blocking, core sensitive information concealment, encryption of information transmission, virus defense, unified log management, data backup, etc.) in accordance with the industry standards to protect the personal data provided by you, and to prevent the data from being accessed without authorization, publicly disclosed, used, modified, damaged or lost.
- Upon the occurrence of a personal data security incident, we will promptly inform you of the basic situation and possible impact of the security incident, the measures we have taken or will take to deal with the incident, the suggestions you can take to prevent and reduce the risk, and the remedial measures for you. We will promptly inform you of the situation related to the incident by email, letter, phone call, push notification, etc. When it is difficult to inform the subject of personal data one by one, we will take a reasonable and effective way to make a public announcement. At the same time, we will also take the initiative to report the disposition of personal data security incidents in accordance with the requirements of the regulatory authorities.

How we handle minors' personal data

We only provide products or services to users who are at least 18 years old and have the appropriate civil behavioral capacity under Chinese law. Your use of the products or services is deemed to fulfill the aforementioned conditions. We attach great importance to the protection of minors' personal information, and we do not collect personal information directly from minors. If you find that you have inadvertently provided us with personal information of minors, please contact us. We will attempt to delete the personal information as soon as possible.

Update of this Privacy Notice

We may change or modify this privacy notice in the future in order to better provide our services. If such changes or modifications result in a material change in your rights under this privacy notice, we will provide you with prominent notice (this includes sending you emails or text messages, etc.) and obtain your consent.

Colombia

Pursuant to the provisions of art. 8 of Law 1581 of 2012, you have the right to

- know, update and rectify your Personal Data from the Controller or the Processor. This right can be exercised, among other, regarding partial data as well as in respect to data that is incomplete or fractioned, that induces error, or those whose Processing is expressly forbidden or has not been authorized;



- request evidence of the authorization granted to the Controller unless when it is expressly excepted as a requirement for the Processing, pursuant to the provisions of article 10 of law 1581 of 2012;
- be informed by the Controller or the Processor upon request, in respect to the use that has been made of your Personal Data;
- file to the Superintendence of Industry and Commerce complaints for infractions to the provisions of Law 1581 of 2012 as amended, added to or supplemented from time to time;
- revoke the authorization and/or to request the deletion of the specific data, provided that there is no legal or contractual obligation that imposes on you the duty to remain in the database;
- have access, free of charge, to your Personal Data that has been the subject of Processing, at least once per calendar month and whenever there are substantial amendments to the Processing policies.

Procedures you have to follow to exercise your personal data rights

- A. Complaints: You may file complaints regarding the Personal Data kept in Audi's databases, according to the following rules:
- The complaint will be analyzed to verify your identification. If the complaint is made by a person other than you and the capacity of such person is not accredited according to the laws in force, the complaint will be rejected.
 - All the complaints will be resolved in a maximum term of ten (10) business days as from the date in which the same are received. If it is not possible to answer the complaint within said term, you will be informed, expressing the reasons for the delay and informing a date in which the enquiry will be answered, which cannot exceed, in any case, five (5) business days after the expiration of the original term.
- B. Requests: If you consider that the data contained in Audi's databases must be subject to corrections, updates or deletion, or when they notice the alleged breach of any of the duties, you may file a request according to the following rules:
- The requests will be analyzed to verify your identification. If the request is made by a person other than you and the representation thereof is not accredited according to the regulations in force, the request will be rejected.
 - The request must contain the following information: (i) your identification; (ii) contact data (physical and/or electronic address and contact phone numbers); (iii) the documents that accredit your identity, or your representation; (iv) The clear and precise description of the Personal Data regarding which you seek to exercise any of the rights; (v) The description of the facts that lead to the request; (vi) The documents that they intend to enforce; (vii) signature and identification number.
 - If the request is incomplete, Audi shall make a requirement to you, within a term of five (5) days after the receipt of the request, to remedy the defects. If two (2) months lapse from the date of the requirement and you have not given the information required, it shall be construed that you have desisted the request.
 - If the area that receives the request is not competent to answer it, it shall pass it to the relevant area or person within a term of two (2) business days and will inform this situation to the interested party.
 - Once the complete request has been received, a note saying "request being processed" shall be included in the database with the reason thereof, in a term of no more than two (2) business days. Said note must be left in place until the moment in which the claim is decided.
 - The maximum term to answer the request will be fifteen (15) business days as from the day after the date in which it is received. When it is not possible to answer the request within that term, the reasons of the delay shall be informed to the interested party together with the date in which the request will be answered, which under no circumstances can exceed eight (8) business days after the expiration of the first term.
 - You have the right, at all times, to request the deletion of you Personal Data. The deletion implies the total or partial removal of the Personal Data from the Data Bases, according to your request. The deletion



right is not absolute and Audi may refuse the exercise thereof in the following events: (i) If you have a legal or contractual duty to remain in the Database or if the Controller has a legal or contractual obligation that means that it has to keep the Personal Data; (ii) The deletion of the Personal Data would thwart judicial or administrative activities related to fiscal obligations, the investigation and persecution of crimes or the update of administrative sanctions; (iii) The Personal Data is necessary to protect your interests protected by the laws, to perform an action pursuant to the public interest, or to comply with an obligation legally acquired by you or by the Controller.

Authorization: As from the enactment of this Notice, at the time of the collection of Personal Data, Audi shall request the prior authorization from you and you shall be duly informed about the specific purposes of the Processing for which such consent has been obtained, excepting in the case of any one of the exceptions provided in article 10 of Law 1581 of 2012 for such purposes.

Audi may transmit and/or transfer your Personal Data to third parties located in Colombia or abroad, as long as Audi has the prior and express authorization of you of the Personal Data.

Retention period: The information provided by you shall only be used for the purposes herein established. Once the need for the Processing of the Personal Data has ceased, the same shall be deleted from Audi's databases.

France

To the extent that the access to the data and the data processing fall within the scope of the data protection laws of France, in addition to the rights listed in Sec. B. IV. you also have the right to define directives concerning the fate of your personal data after your death (post-mortem right).

Hong Kong

In addition to your rights set out in Sec. 4, you may withdraw your consent to the use of your personal data.

In addition to your rights set out in Sec. 4, you will be informed at the time of the first communication with you in direct marketing without charge to you.

India

You have the right to

- access;
- rectification;
- withdraw consent;
- contact the Grievance Officer. The Data Protection Officer is the Grievance Officer for Audi. For the contact details please see Sec. 3.

Israel

You have the right, subject to Protection of Privacy Law, 5741-1981 and the regulations enacted therefrom, to

- be informed if you are under a legal duty to provide the data, the purpose of collection, and details of any third party that will receive the data and for what purpose;
- access;

Anex 1: Additional data subject rights and further country-specific information



- rectification: request correction of the inaccurate or missing data or request deletion or destruction of the data;
- object to the processing (e.g. if the data is being unlawfully processed).

Japan

You have the right to

- request information on purpose of use;
- request information on security control measures;
- request access;
- request correction, addition or deletion;
- request discontinuance of use or erasure; and

request explanations on data processing.

Kuwait

Legitimate interest is not recognized as a valid legal basis for data processing in Kuwait. You have the right to

- grant or withhold your consent to the collection and processing of your personal data. Prior to providing your consent, you should be notified of the purpose for the collection and processing of your personal data;
- access, rectify, transport and update the data;
- request omission or erasure if you withdraw your consent.

Data controllers and data processors are similarly treated under Kuwait law when they collect personal data. For purposes of data protection, they are subject to the same duties and liabilities.

Malaysia

You have the right to

- request access to your personal data;
- request correction of your personal data;
- prevent processing likely to cause damage or distress; and
- prevent processing for purposes of direct marketing.

Upon exercising your rights stated above in written form addressed to the contact details listed in Sec. 1., if you are dissatisfied with our response or we fail to provide a response within 21 days of receipt, you have the right to submit an application to the Personal Data Commissioner to require us to comply with your request. The application to the Personal Data Commissioner can be made to the following address:

Commissioner of Personal Data Protection, 6 th Floor, KKMM Complex Lot 4G9, Persiaran Perdana, Presint 4 Federal Government Administrative Centre 62100 Putrajaya.



Mexico

You have the right to:

- access;
- rectify;
- cancel;
- oppose;
- file data protection measures with the Federal Institute for Access to Information and Data Protection;
- request a reconsideration of a decision made via automated decision making in case you are of the opinion that the data processed in this context is (partly) incomplete or incorrect.

Morocco

In addition to your rights set out in Sec. B.IV, you have the following rights under Moroccan Law No. 09-08 on the protection of individuals with regard to the processing of personal data:

- access your personal data;
- rectification of inaccurate or incomplete personal data;
- erasure of personal data, subject to legal retention obligations;
- object, at any time, to the processing of your personal data on legitimate grounds;
- object to the processing of your personal data for direct marketing purposes;
- withdraw your consent at any time where processing is based on consent;
- be informed about the processing of your personal data, including categories, purposes, and recipients;

lodge a complaint before the Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) if you believe your rights have been infringed.

New Zealand

You have the right to

- know what personal data is held;
- request for personal data held and access the personal data;
- rectification;
- a response to your request within 20 working days, if you make a request for access to or rectification of your personal information. In limited circumstances, Audi may extend this 20 working day time limit, but we must tell you the period of the extension and the reasons for the extension.
- lodge a complaint with both Audi and the Privacy Commissioner. However, it is a requirement that before you can complain to the Privacy Commissioner you must first raise your complaint with Audi. If you are not satisfied with Audi's response or you do not receive a response, you can lodge a complaint to the Privacy Commissioner. In general, you should wait at least 30 working days for a response before contacting the Privacy Commissioner to lodge a complaint.



Qatar

In addition to your rights set out Sec. 4 you have further rights under local Qatari data protection law.

Processing of sensitive personal data requires authorization from Qatar's National Cyber Security Agency Pursuant to Article 16 of Qatar Law No. 13 of 2016 (Qatar's Protection Data Protection Law).

You have the right to object to the processing of your personal data if we process your data for direct marketing purposes, or if such processing is not necessary to achieve the purposes for which such personal data has been collected or where such collected personal data is proven in excess of the amount required, discriminatory, unfair or illegal, as well as the right to request omission or erasure if you withdraw your consent.

Oman

You have the right to

- revoke your consent to the processing of your personal data, without prejudice to the processing that took place prior to the revocation;
- request to have your personal data amended, updated, or blocked;
- obtain a copy of your processed personal data;
- transfer your personal data to another controller;
- request the erasure of your personal data unless such processing is necessary for the purposes of national archiving and documentation;
- request that the processing of your personal data be suspended until any of the foregoing requests are decided upon by the controller;
- be notified of any breach or infringement of your personal data, and of the actions taken in this regard;
- submit a complaint or a report to the competent administration for any violation by the controller on the form prepared for this, within a maximum period of 30 (thirty) days from the date of certain knowledge of the violation.

Legitimate interest is not recognized as a valid legal basis for the collection and processing of personal data under the laws of Oman. Accordingly, in situations where Audi would typically rely on legitimate interest or a legitimate interest to justify processing, an alternative legal basis would be required in Oman.

Saudi Arabia (KSA)

You have the statutory right under the Saudi Arabia Cabinet Decision No. 98/1443 (the "PDPL") to:

- Be informed about the collection, purpose, legal basis, retention period, and mandatory/optional nature of your personal data, including how to exercise your rights and revoke consent.
- Access your personal data held by Audi, taking into account the rights of others
- Receive a copy of your personal data in a clear, readable, and commonly used electronic format, or printed format where possible.
- Request correction, completion, or updating of any inaccurate or incomplete personal data
- Request the destruction of personal data that is no longer necessary, subject to statutory requirements.

Legal guardians may exercise these rights on behalf of incompetent or incapacitated individuals.

Audi has the right to refuse repeated or manifestly excessive requests with justification.

Anex 1: Additional data subject rights and further country-specific information



Audi will adopt the necessary technical, administrative, and organizational measures to ensure a prompt response to requests and proper documentation, including verbal requests.

Audi may transfer personal data to recipients outside the Kingdom of Saudi Arabia only in accordance with the PDPL and its implementing regulations. Such transfers will be conducted with appropriate safeguards to ensure an adequate level of protection for personal data, not less than that prescribed by the law and regulations.

Appropriate safeguards may include:

- Standard contractual clauses approved by the competent authority;
- Binding corporate rules; or

Certification of accreditation.

Serbia

You have the right to be informed about appropriate safeguards in case of a data transfer to countries or international organisations outside Serbia that do not provide an adequate level of data protection recognised by a Serbian Government Decision. All EU / EEA Member states provide an adequate level of data protection recognised by a Serbian Government Decision.

You have the right to file a complaint regarding the processing of your personal data at the Commissioner for Information of Public Importance and Personal Data Protection (<https://www.poverenik.rs/sr-yu/kontakt.html>), as the supervisory authority for personal data protection in the Republic of Serbia.

Contact person for exercising your rights:

If you wish to exercise your rights in relation to the processing of your personal data, you can contact us using the contact details above or via the authorized local contact person using the contact details below:

PORSCHE SCG DOO BEOGRAD
Zrenjaninski put 9a
11210 Beograd
Serbia

Email: zastita.podataka@porschescg.rs

Singapore

You have statutory rights as provided under Singapore's Personal Data Protection Act 2012, including the rights to

- request access to your personal data;
- request correction of your personal data; and
- withdraw consent to the collection, use or disclosure of your personal data (where applicable), subject to any grounds for the collection, use or disclosure without your consent that are required or authorised under the Personal Data Protection Act 2012 or any other written law of Singapore.

South Africa

You have the right to

- not have your personal data processed for the purposes of direct marketing by unsolicited electronic communication;
- initiate civil proceedings;

Anex 1: Additional data subject rights and further country-specific information



- be informed if your personal information has been compromised;
- be informed, free of charge and before the information is included in a directory, should you be a subscriber to a printed or electronic directory;
- lodge a complaint to the Information Regulator of South Africa by completing this [form](#) and sending it to POPIAComplaints@inforegulator.org.za

For further information about your South African data privacy rights, please click [here](#) which will take you to the website of the Information Regulator.

South Korea

You (and your legal representative) have statutory rights under the Korean Personal Information Protection Act, in particular the right to

- access;
- rectification / erasure;
- suspension of processing; and
- withdrawal of consent.

You (or your legal representative) can exercise such rights by contacting us or our data protection officer using the contact details set out in Sec. 3.

Certain personal data may be retained for compliance with local laws and regulations for certain periods, such as the following:

- All transaction records and relevant documentary evidence as prescribed by applicable tax laws: 5 years (as required under the Framework Act on National Taxes and the Corporate Tax Act)
- Records of logins: 3 months (as required under the Protection of Communications Secrets Act)
- Records on labels and advertisements: 6 months (as required under the Act on Consumer Protection in Electronic Commerce)
- Records on revocation of contracts or cancellation of orders/purchases, payments, provision of products and services: 5 years (as required under the Act on Consumer Protection in Electronic Commerce)
- Records on handling of customer complaints or disputes: 3 years (as required under the Act on Consumer Protection in Electronic Commerce)

The process and method for destroying personal data are set forth below.

- Process of destruction: We select the relevant personal data to be destroyed and destroy it with the approval of our Data Protection Officer.
- Method of destruction: We destroy personal data recorded and stored in the form of electronic files by using a technical method (e.g., low level format) to ensure that the records cannot be reproduced, while personal data recorded and stored in the form of paper documents shall be shredded or incinerated

If it is necessary to retain personal data for a period longer than the legal retention periods described herein, to the extent required by the laws of the applicable country, we shall obtain the data subject's consent for such longer retention of personal data.

Spain

To the extent that access to and processing of data falls within the scope of data protection laws of Spain, please note that your personal data will be deleted after the statutory retention period has expired if the legal basis for processing

Anex 1: Additional data subject rights and further country-specific information



your personal data no longer applies (in particular if you withdraw your consent), if the processing of your personal data is no longer necessary for the respective purpose or if the purpose itself no longer applies.

Switzerland

To the extent data processing falls within the scope of the Swiss Federal Act on Data Protection (FADP), (a) the scope of "personal data" shall be determined in accordance with the FADP, and (b) references to the GDPR shall be understood as references to the FADP.

In addition or rather supplementary to your rights listed above under B. VII. the following applies.

You have the right to file a complaint regarding the processing of your personal data at the Swiss Federal Data Protection and Information Commissioner (FDPIC) <https://www.edoeb.admin.ch/edoeb/en/home.html>.

Taiwan

You have the right to

- make an inquiry of and to review your personal data;
- request a copy of your personal data;
- supplement or correct your personal data;
- demand the cessation of the collection, processing or use of your personal data; and
- erase your personal data.

Thailand

Please note that your right to obtain a copy of the personal data is subject to law or pursuant to a court order, and must not adversely affect the rights and freedoms of others.

Turkiye

You have statutory rights under Art. 11 of the Turkish Data Protection Law, in particular the right to

- request reporting of the operations carried out which are rectification of the incomplete or inaccurate data, if any and the erasure or destruction of your personal data) to third parties to whom your personal data have been transferred;
- claim compensation for the damage arising from the unlawful processing of your personal data;
- object to the occurrence of a result against yourself by analyzing the data processed solely through automated systems;
- lodge a complaint with the Turkish Data Protection Authority (Kişisel Verileri Koruma Kurumu) Nasuh Akar Mahallesi 1407. Sok. No:4, 06520 Çankaya/Ankara/Turkiye.

The objection can be exercised in the forms stated in Article 5/1 of the Communiqué On The Principles and Procedures for the Request To Data Controller.

Local representative:

Doğuş Otomotiv Servis ve Ticaret A.Ş.
Şekerpınar Mahallesi, Anadolu Cad. No:22 Çayırova/Kocaeli - Mersis No: 0-3090-1147-1300010
Telephone number: +90 (0) 262 676 90 90



United Arab Emirates

Legitimate interest is not recognized as a valid legal basis for the collection and processing of personal data under the PPD. Accordingly, in situations where Audi would typically rely on legitimate interest or a legitimate interests to justify processing, an alternative legal basis would be required in the UAE.

Your Rights to correct, erase, restrict, or object to processing

Under the Federal UAE Data Protection Law (the “PPD”), you may at any time exercise your rights of rectification, erasure, restriction, or objection by submitting a written request to Audi through our dedicated communication channels. Upon receiving your request, we will verify your identity, assess the legitimacy of your request against the statutory grounds, and respond without undue delay.

Right to correct your personal data: you may request the correction or completion of the personal data held with Audi without undue delay.

Right to erase your personal data: without prejudice to the legislation in force or what is required by the public interest, you may request the erasure of your personal data held with Audi in the following cases:

Your personal data is no longer required for the purposes for which it is collected or processed.

You have withdrawn your consent on which processing is based.

You object to the processing or if there are no legitimate reasons for Audi to continue the processing.

The processing of your personal data is in violation of the PPD and applicable legislation and the erasure process is necessary to comply with applicable legislation.

With the exception of what is stated in Item (b), you have no right to request the erasure of your personal data held by Audi if:

The request is for the erasure of personal data related to public health and held with private establishments.

The request affects investigation procedures, claims for rights and legal proceedings or defense by Audi.

The request conflicts with other legislation to which Audi is subject.

The request conflicts with other cases set by the Executive Regulations of the PPD.

Right to restrict processing: you have the right to oblige Audi to restrict and stop processing in any of the following cases:

If you object to the accuracy of your personal data, in which case the processing shall be restricted to a specific period allowing Audi to verify accuracy of the data.

If you object to the processing of your personal data in violation of the agreed purposes.

If the processing is made in violation of the PPD and the legislation in force.

Notwithstanding the foregoing provisions “Right to restrict processing”, Audi may proceed with the processing of your personal data without your consent in any of the following cases:

if the processing is limited to storing your personal data

if the processing is necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial procedures.

if the processing is necessary to protect the rights of third parties in accordance with the legislation in force.

if the processing is necessary to protect the public interest.

Right to stop processing: you have the right to object to and stop the processing of your personal data in the following cases:

The processing is for direct marketing purposes including profiling related to direct marketing.



The processing is for the purposes of conducting statistical surveys unless the processing is necessary to achieve the public interest.

The processing is in violation of the processing controls mandated by the PPD.

Our actions in the event of a data breach or violation of the PPD

If we become aware of any personal data breach or other infringement of the PPD that compromises the confidentiality, integrity, or availability of your personal data, we will immediately activate our incident response procedure. Without delay, and within the specific timeframe set in the Executive Regulations, we will notify the UAE Data Office, providing details such as the nature, scope, and root cause of the breach; categories and approximate number of affected records and individuals; contact details of our Data Protection Officer; likely consequences; remedial and mitigation measures already taken or proposed; and full documentation of the event.

Where the breach is likely to result in a serious risk to your privacy, we will also notify you, describing the breach in clear language and advising you on protective steps. At the same time, we will isolate the incident, contain further exposure, preserve forensic evidence, and implement technical and organisational measures to prevent recurrence. In the event of any violation of the PPD, whether identified internally or following a regulatory inquiry, we will cooperate fully with the UAE Data Office, undertake a root-cause analysis, update our policies, and, where necessary, conduct a data-protection impact assessment to validate continued compliance.

United Kingdom

To the extent data processing falls within the scope of the UK General Data Protection Regulation (UK GDPR) references to GDPR, in particular legal basis, shall be understood as references to the UK GDPR.

You have the right to file a complaint regarding the processing of your personal data or handling your data subject's rights requests at Audi by following the same process for submitting a request and include "complaint" in your request. Subsequently, if Audi denies your complaint or does not acknowledge the complaint within 30 days, you may contact the UK Information Commissioner's Office (ICO): <https://ico.org.uk/global/contact-us/>

Vietnam

In addition to your rights set out in Sec. B.IV, you have the following rights under the Vietnamese Personal Data Protection Decree (Decree 13/2023/ND-CP):

- access your personal data;
- rectification;
- erasure, subject to statutory retention requirements;
- restriction of processing;
- object to the use or disclosure of your personal data;
- withdraw your consent at any time and free of charge;
- be informed about the processing of your personal data, including sensitive personal data;
- request the provision of your personal data to competent authorities where required by law;
- lodge a complaint before the competent Vietnamese authorities regarding the processing of your personal data;

receive information about international transfers of your personal data originating from Vietnam, including the required Data Transfer Impact Assessment prepared in accordance with Vietnamese law.



Version	Responsible	Description of changes
06/2026	I/BZ-Z	• Detailed description of the processed data • Further specification of data processing under the sole responsibility of Audi • Integration Japan specific regulations (in the past own privacy documents) • Addition of new countries (Middle East): Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, UAE, as well as China, France, Spain, Switzerland, United Kingdom, Morocco, Vietnam • Supplement for South Korea: details regarding the domestic agent and inclusion of additional information for Serbia • Editorial revision of the entire document